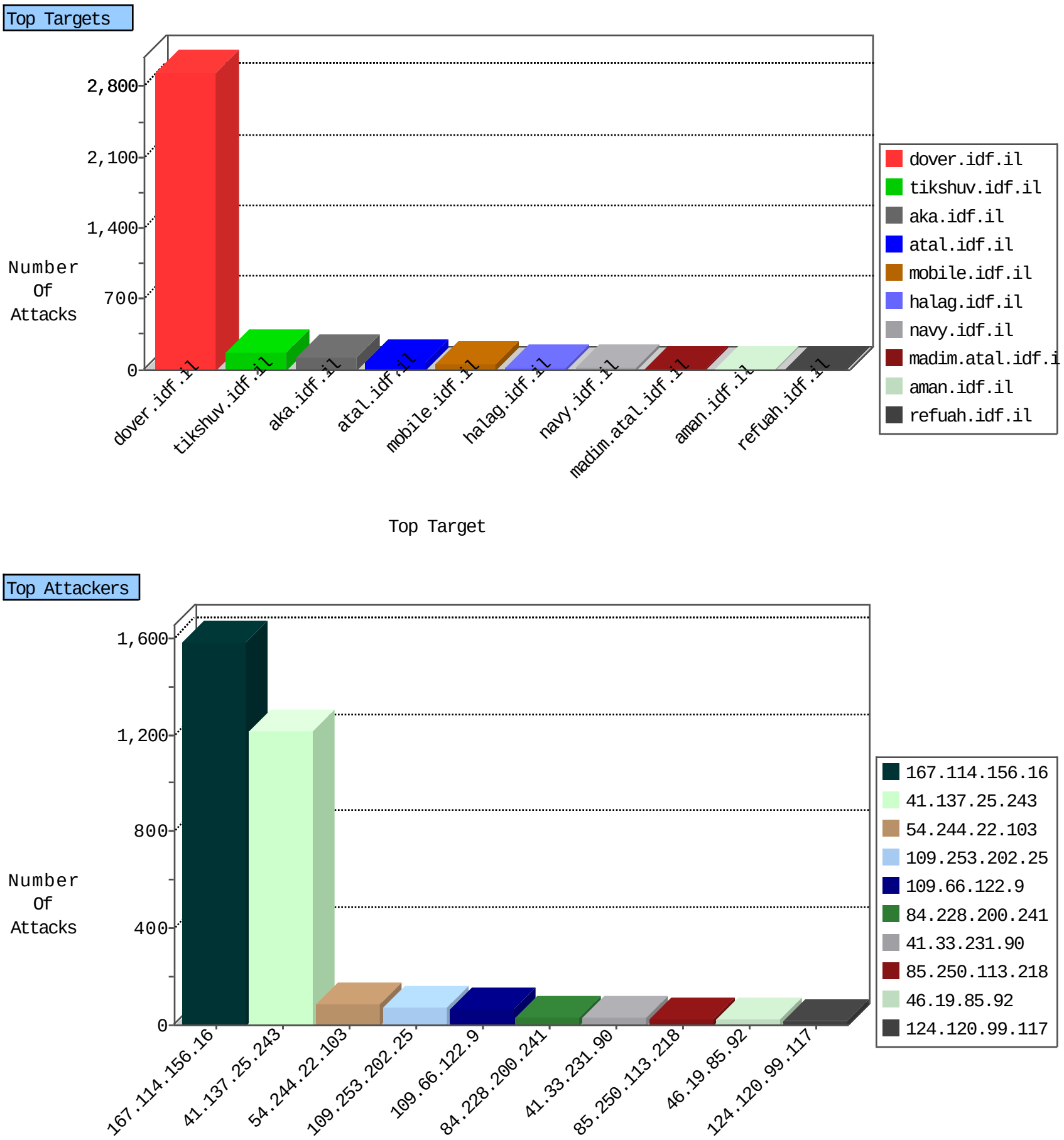
01-11-2016-00:04:07 to 01-11-2016-01:04:07

IDF Under Attack Daily Report



01-11-2016-00:04:07 to 01-11-2016-01:04:07

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	3006
41.137.25.243	Morocco	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Http	drop	2
46.228.207.18	Germany	147.237.76.197	e.himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
134.147.203.115	Germany	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	2
41.137.25.243	Morocco	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
23.95.248.111	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

01-11-2016-00:04:07 to 01-11-2016-01:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
40.77.167.42	United States	147.237.77.216	dover.idf.il	C1000158: HTTP(S): Hacked in the Payload	Block	1
123.126.113.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

01-11-2016-00:04:07 to 01-11-2016-01:04:07

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
109.253.202.25	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
66.102.9.21	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
40.77.167.42	147.237.77.216	United States	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	1
5.39.222.196	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.39.222.196	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
193.105.134.220	147.237.0.33	Sweden	idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.247	147.237.0.17		m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
77.109.38.223	147.237.77.205	Ukraine	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.77.216	Germany	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.76.200	Germany	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.76.44	Germany	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.39.222.196	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.39.222.196	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.247	147.237.76.197		e.himush.idf.il	ET SCAN Potential SSH Scan	1
46.228.207.18	147.237.77.216	Germany	dover.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.76.176	Germany	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

01-11-2016-00:04:07 to 01-11-2016-01:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.137.25.243	Morocco	147.237.77.216	dover.idf.il	drop	SAM rule	drop	151
54.244.22.103	United States	147.237.0.34	tikshuv.idf.i	drop	First packet isn't SYN	drop	86
109.253.202.25	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	32
109.253.202.25	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
84.228.200.241	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
41.137.25.243	Morocco	147.237.77.216	dover.idf.il	drop		drop	17
124.120.99.117	Thailand	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
2.54.130.213	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
41.137.25.243	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
185.32.179.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
5.102.254.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.92	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.180.223.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
79.180.223.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.66.122.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.137.25.243	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
217.132.135.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.146.144	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
131.191.68.76	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
217.132.135.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.66.12.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	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
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
79.177.208.137	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.46.46.204	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.102.253.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.254.184	Israel	147.237.72.156	aman.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
5.28.147.205	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
41.137.25.243	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.181.22.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.249.245	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	3
124.120.99.117	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
87.69.4.210	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.180.133.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.0.207	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.70	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
50.18.94.121	United States	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
185.3.147.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
213.8.204.55	Israel	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
195.60.232.57	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
84.228.232.54	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
185.3.147.239	Israel	147.237.0.34	tikshuv.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
79.181.100.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

01-11-2016-00:04:07 to 01-11-2016-01:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.137.25.243	Morocco	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	512
41.137.25.243	Morocco	147.237.77.216	dover.idf.il	Multiple Malformed URL from 41.137.25.243	Block	508
109.66.122.9	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 109.66.122.9	Block	61
85.250.113.218	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	25
5.28.147.205	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 5.28.147.205	Block	8
109.253.202.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.54.130.213	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
37.26.146.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.121.138.141	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	3
84.108.12.183	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
185.120.125.15		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
149.78.249.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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	2
217.118.64.59	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20707-he/dover.aspx	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
61.135.190.69	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/reset.css	Block	1
109.253.202.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
89.138.191.130	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.47	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/about/pages/structure.aspx	Block	1
61.135.190.198	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/shared/clientscripts/sa_swfobject.js	Block	1
109.253.133.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.53.4	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
217.132.135.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.144.19	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.183	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.10	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/brothers/skira/default.asp-catid=57479&docid=	Block	1
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
61.135.190.71	China	147.237.0.15	kosher-kravi.idf.i	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
40.77.167.43	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/links.aspx	Block	1
213.8.204.55	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.8.204.55	Block	1
79.177.53.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
176.10.104.243	Switzerland	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
61.135.190.200	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/layout.css	Block	1
46.19.85.92	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.253.140.168	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.200.241	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.69.38	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1730	Block	1
207.46.13.10	United States	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/sachar/faq/outerfaq.asp	None	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/core/doc_mgr/mazi.idf.il	Block	1
61.135.190.71	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/layout2.css	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
40.77.167.55	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/s/psearch/fod_ranking.aspx	Block	1
213.8.204.55	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/3/	Block	1
79.180.223.82	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.219.154.165	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1

01-11-2016-00:04:07 to 01-11-2016-01:04:07