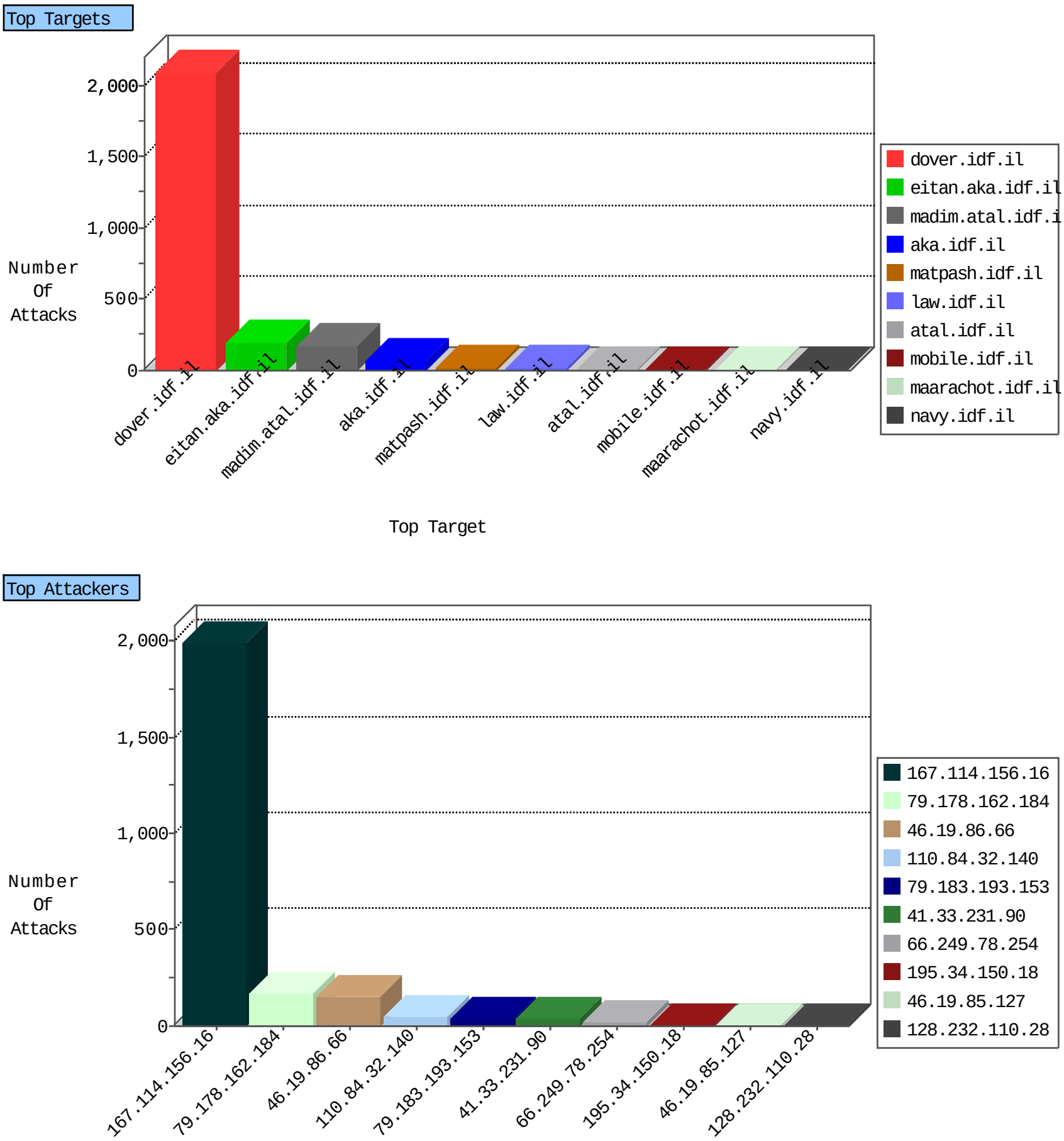
01-22-2016-01:06:11 to 01-22-2016-02:06:11

IDF Under Attack Daily Report



01-22-2016-01:06:11 to 01-22-2016-02:06:11

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	3067
115.239.228.10	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Http	drop	2
31.168.214.8	Israel	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
31.168.214.8	Israel	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1
31.168.214.8	Israel	147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1

01-22-2016-01:06:11 to 01-22-2016-02:06:11

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
110.84.32.140	China	147.237.77.74	law.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	8
110.84.32.140	China	147.237.77.233	atal.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	4
110.84.32.140	China	147.237.77.170	maarachot.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	4
110.84.32.140	China	147.237.77.176	matpash.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	4
110.84.32.140	China	147.237.77.226	www.chamatz.aka.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	3
110.84.32.140	China	147.237.77.234	halag.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	3
110.84.32.140	China	147.237.77.216	dover.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	2

01-22-2016-01:06:11 to 01-22-2016-02:06:11

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
88.204.187.90	147.237.77.205	Kazakstan	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
88.204.187.90	147.237.77.205	Kazakstan	prisha.idf.il	ET SCAN NMAP -f -sS	1
218.246.0.97	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
108.168.185.133	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
88.204.187.90	147.237.77.205	Kazakstan	prisha.idf.il	ET SCAN NMAP -sS window 1024	1

01-22-2016-01:06:11 to 01-22-2016-02:06:11

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.66	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	150
79.183.193.153	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
66.249.78.254	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
110.84.32.140	China	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.60.42.63	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
82.145.211.23	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.120.128.75	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.22.130.102	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.215	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.228.162.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.130	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.83.155	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
66.249.66.69	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
121.54.44.95	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
110.84.32.140	China	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
128.232.110.28	United Kingdom	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
40.77.167.57	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
141.212.121.192	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.19.85.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
110.84.32.140	China	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
84.108.137.22	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	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
128.232.110.28	United Kingdom	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
62.210.181.15	France	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
84.110.184.55	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
128.232.110.28	United Kingdom	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
42.62.74.80	China	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
110.84.32.140	China	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
82.145.211.23	Europe	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.50.77.72	Switzerland	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.142.191.219	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.110.184.55	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
79.78.63.5	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.8.204.63	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.119	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
130.193.51.37	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.85.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
66.249.66.75	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
46.19.86.33	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
79.176.16.42	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.60.232.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

01-22-2016-01:06:11 to 01-22-2016-02:06:11

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.162.184	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	93
79.178.162.184	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.178.162.184	Block	73
110.84.32.140	China	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 110.84.32.140	Block	3
79.177.152.57	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 79.177.152.57 (Unknown SSL Session)	None	2
110.84.32.140	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 110.84.32.140	Block	2
80.178.17.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
110.84.32.140	China	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 110.84.32.140	Block	2
79.177.169.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
208.115.113.92	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
66.249.66.72	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/templatecontrols/generic/	Block	1
195.62.53.168	Russian Federation	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to /login	Block	1
31.168.197.195	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
167.114.0.27	Canada	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/brothers/skira/default.asp	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	1
188.138.9.49	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.120.56.7	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
2.52.39.51	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.8.204.55	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
66.249.69.89	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1404-he/atal.aspx	Block	1
195.62.53.168	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /login	Block	1
37.128.186.113	United Kingdom	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/test/wp-admin/	Block	1
176.205.43.127	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.177.152.57	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
190.42.40.176	Peru	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.120.56.7	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
5.29.2.229	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
110.84.32.140	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/editor/editor/filemanager/browser/default/connectors/asp/connector.asp	Block	1
213.8.204.55	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/xmlrpc.php	Block	1
197.40.177.226	Egypt	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
176.205.43.127	United Arab Emirates	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
40.77.167.63	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/index/	Block	1
109.200.5.149	United Kingdom	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wordpress/wp-admin/	Block	1
207.46.13.122	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
79.177.152.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
191.252.48.220	Brazil	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/old/wp-admin/	Block	1
54.166.46.37	United States	147.237.77.74	law.idf.il	Illegal Byte Code Character in URL /261-6858-en/patzar.aspx	Block	1
5.29.2.229	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
86.143.101.138	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
66.249.78.161	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
197.40.177.226	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
180.210.204.141	Singapore	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wp/wp-admin/	Block	1
46.19.85.168	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
109.253.207.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.129	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/civiladministration/minhalnews/pages/hakalahom.aspx	Block	1
192.114.91.215	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1

01-22-2016-01:06:11 to 01-22-2016-02:06:11