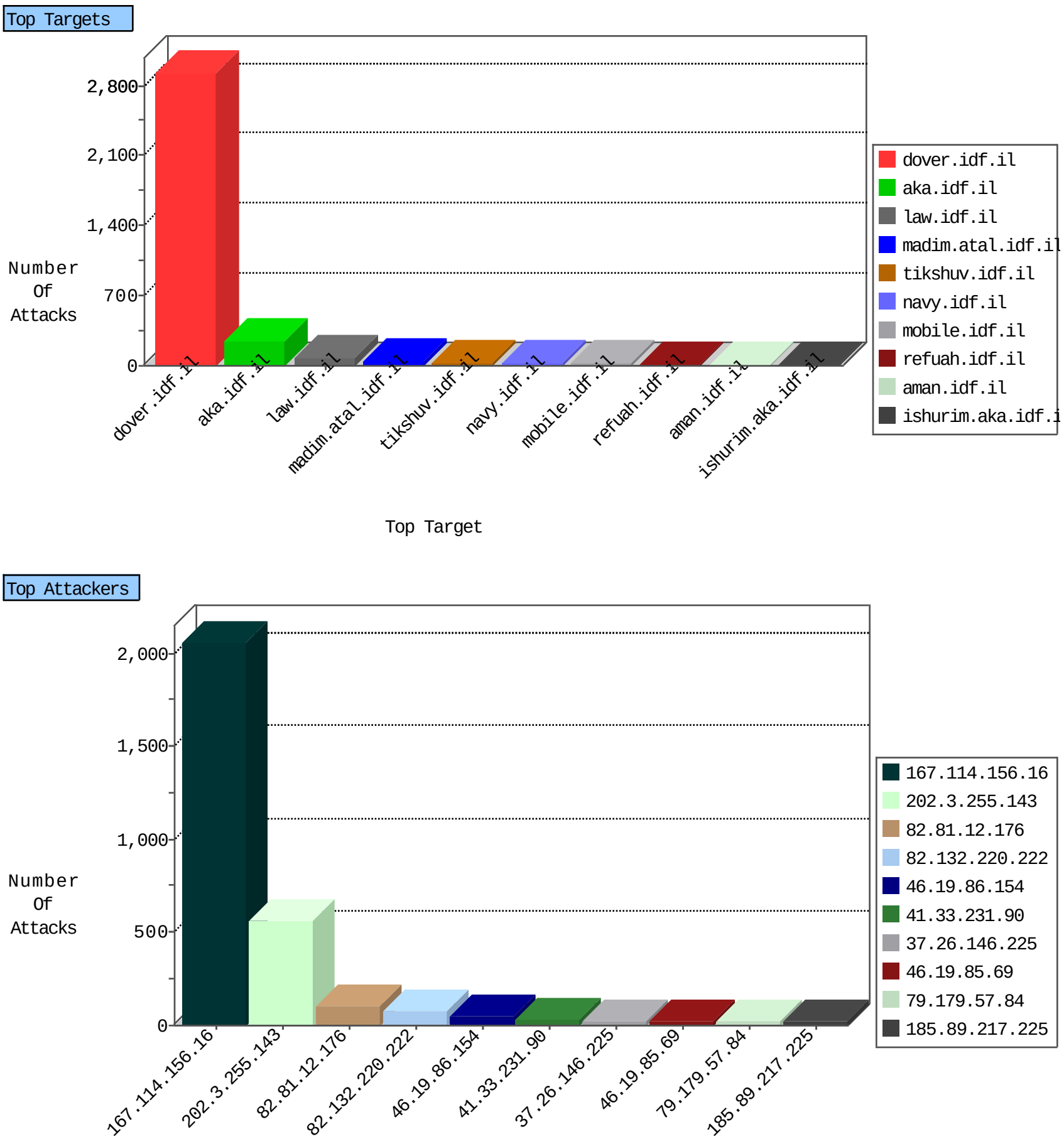
01-20-2016-00:04:03 to 01-20-2016-01:04:03

IDF Under Attack Daily Report



01-20-2016-00:04:03 to 01-20-2016-01:04:03

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	3176
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	106
82.132.220.222	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
37.26.146.225	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
109.66.117.127	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
82.132.220.222	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
207.46.13.49	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
207.46.13.193	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
185.35.62.216	Switzerland	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
185.35.62.100	Switzerland	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
45.35.64.142		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
197.48.141.104	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
185.35.62.162	Switzerland	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
71.6.135.131	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.211	Switzerland	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1

01-20-2016-00:04:03 to 01-20-2016-01:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.223.18.84	Spain	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	2
91.121.169.194	France	147.237.0.34	tikshuv.idf.il	C106: HTTP: majestic bot	Block	2
91.121.169.194	France	147.237.77.74	law.idf.il	C106: HTTP: majestic bot	Block	2
2.54.141.221	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
157.55.39.156	United States	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

01-20-2016-00:04:03 to 01-20-2016-01:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	518
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.234	147.237.0.34		tikshuv.idf.il	ET SCAN Potential SSH Scan	1
201.232.25.160	147.237.77.179	Colombia	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
201.232.25.160	147.237.77.179	Colombia	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
198.11.178.114	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
190.249.184.162	147.237.77.121	Colombia	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
185.130.5.234	147.237.77.170		maarachot.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.234	147.237.76.198		e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.234	147.237.76.176		test.ncore.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.234	147.237.0.200		m4u.idf.il	ET SCAN Potential SSH Scan	1
201.232.25.160	147.237.77.179	Colombia	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
198.11.178.114	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 4096	1
185.130.5.234	147.237.77.216		dover.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.234	147.237.77.74		law.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.234	147.237.76.196		e.sviva.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.234	147.237.72.217		e.idf.il	ET SCAN Potential SSH Scan	1

01-20-2016-00:04:03 to 01-20-2016-01:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
82.132.220.222	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
82.132.220.222	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
31.210.188.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
79.178.178.231	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
2.54.48.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.179.57.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.89.217.225		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.52.6.102	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
185.89.217.224		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	9
82.132.220.222	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
197.48.141.104	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.222	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.152.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.1.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.222	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.78.240.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.1.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.69	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.146.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
82.132.220.222	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.69	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	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
37.26.146.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.210.187.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.146.225	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
79.179.57.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	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
176.13.8.178	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.89.217.226		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.230		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.22.131.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.89.217.228		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.235		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
5.22.135.60	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.8	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.160.175.99	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.121.120.173	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
79.179.62.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.154	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.152.97	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.175.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.86.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

01-20-2016-00:04:03 to 01-20-2016-01:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
66.249.93.117	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 66.249.93.117	Block	15
109.66.169.27	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1403	Block	6
109.66.184.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.52.6.102	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
149.78.175.19	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.229.35.172	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
213.8.204.60	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.148.215	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
79.179.188.98	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
52.49.9.185	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.1.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.190.61	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19149-he/dover	Block	1
85.65.8.124	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/resource/userfollowresource/create/	Block	1
37.228.225.80	Ireland	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.182.62.132	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
52.90.211.233	United States	147.237.76.86	navy.idf.il	Directory Traversal (In URL)	Block	1
185.89.217.230		147.237.77.74	law.idf.il	URL is Above Root Directory www.law.idf.il/../images/1.he/navigation/navigation_arrow.gif	Block	1
5.255.253.62	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.172.160.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
72.37.140.46	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
46.19.85.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
141.212.122.177	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
80.246.136.122	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
52.90.211.233	United States	147.237.76.86	navy.idf.il	Directory Traversal - 16	Block	1
207.46.13.88	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/kamlar/klali/default.asp	None	1
31.168.72.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.68.110	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/1119-he/nakhal.aspx&sa=u&ved=0ahukewi9jtnu-rbkahxdfywkhybfdswqfggrmam&usg=afqjcngfdy61nzfm6uzvc64ixqbk9dkbia	Block	1
79.179.96.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.45.118	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
83.130.106.49	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
62.219.92.189	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
208.80.155.130	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar	Block	1
37.26.146.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.65.13.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.183.197	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	1
5.22.131.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.93.117	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1

01-20-2016-00:04:03 to 01-20-2016-01:04:03