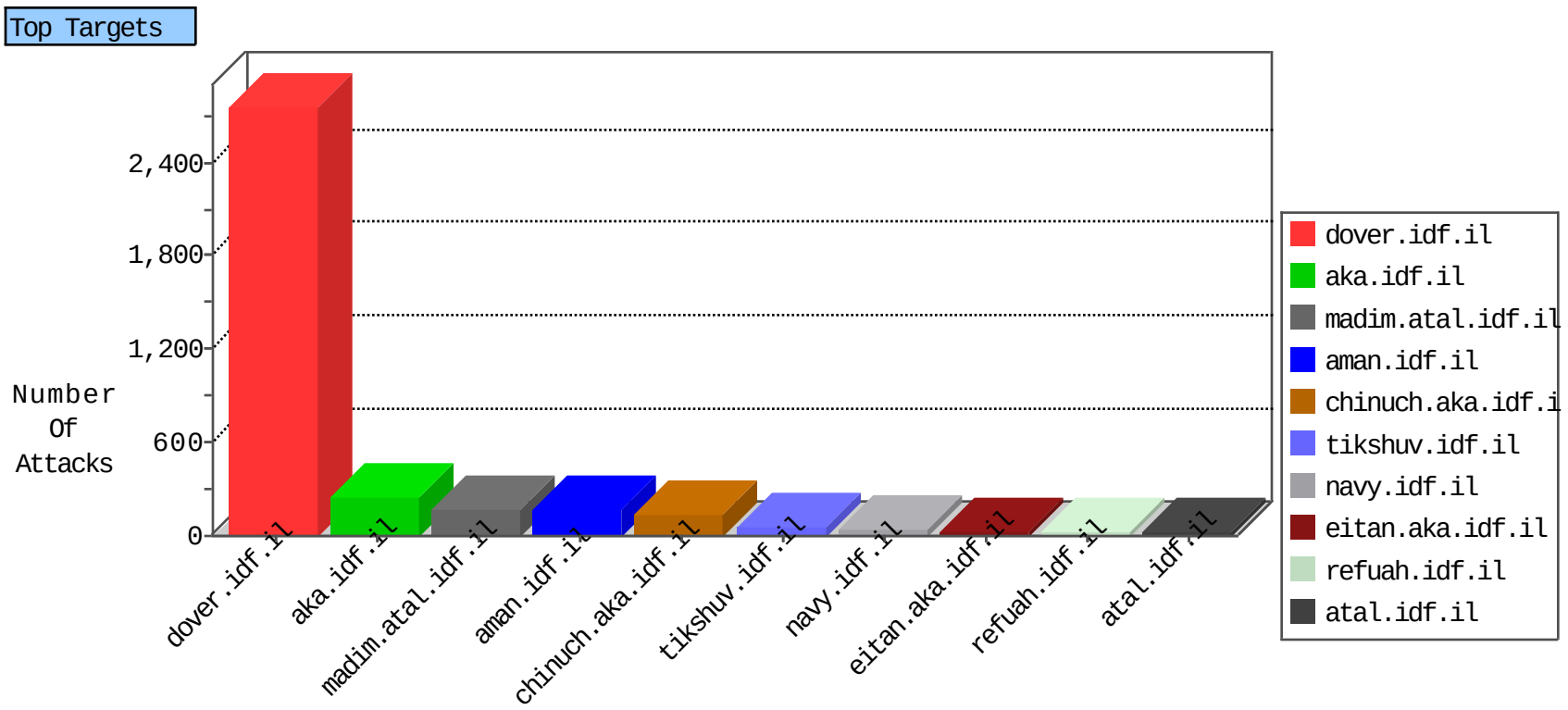
03-16-2016-17:04:02 to 03-16-2016-18:04:02

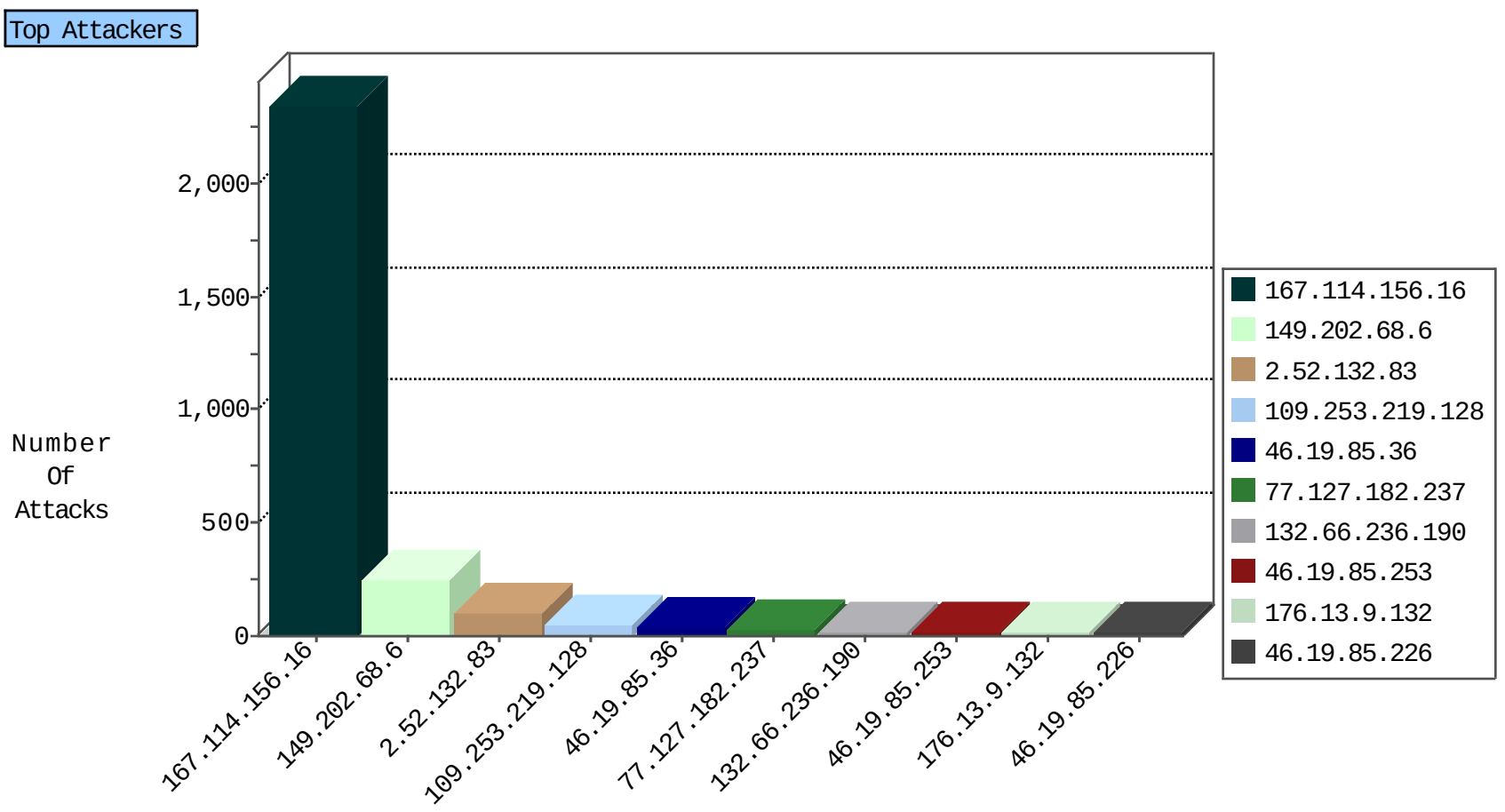
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

03-16-2016-17:04:02 to 03-16-2016-18:04:02

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	3286
194.165.134.84	Jordan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
82.145.209.121	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	3
66.240.219.146	United States	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
149.165.249.151	United States	147.237.76.86	navy.idf.il	L4 Source or Dest Port Zero	drop	1
82.145.211.123	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1

03-16-2016-17:04:02 to 03-16-2016-18:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.38.189	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
149.88.249.228	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.253.194.115	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
84.108.89.157	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
79.182.30.212	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
2.54.154.251	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
176.9.131.69	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-16-2016-17:04:02 to 03-16-2016-18:04:02

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	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
185.130.5.208	147.237.77.61		e.cogat.idf.il	ET SCAN Potential SSH Scan	1
46.120.97.238	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.208	147.237.76.200		eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.233.114	147.237.8.24		e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.208	147.237.76.38		e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
41.228.12.4	147.237.76.202	Tunisia	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
185.130.5.208	147.237.0.15		kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
41.228.12.4	147.237.0.200	Tunisia	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
185.120.125.43	147.237.72.166		aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.64.0	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
162.243.40.70	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
37.139.27.231	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.72.14	United States	dover.idf.il(old)	ET DROP Dshield Block Listed Source	1
149.88.239.54	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.165.134.84	147.237.77.216	Jordan	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.164.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.208	147.237.77.235		sviva.idf.il	ET SCAN Potential SSH Scan	1
66.240.213.93	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.208	147.237.76.200		eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
46.117.69.100	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.208	147.237.76.148		gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
41.228.12.4	147.237.76.202	Tunisia	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
185.130.5.208	147.237.72.217		e.idf.il	ET SCAN Potential SSH Scan	1
41.228.12.4	147.237.76.202	Tunisia	e.halag.idf.il	ET SCAN NMAP -f -sS	1
185.120.126.162	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.19.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.139.27.231	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
162.243.40.70	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
37.139.27.231	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.219.234	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.126.77.138	147.237.77.226	Sweden	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.66.81	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1

03-16-2016-17:04:02 to 03-16-2016-18:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.202.68.6	Germany	147.237.72.156	aman.idf.il	SYN Attack		reject	79
149.202.68.6	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	69
149.202.68.6	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	46
149.202.68.6	Germany	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	43
77.127.182.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
132.66.236.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
46.19.85.253	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.86.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.94.100.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
213.8.159.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
149.202.68.6	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.52.25.109	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.121.128.148	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.172	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.61	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.166.72	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.85.187	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.226	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
87.70.9.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.219.128	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.65.48.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.180.107.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.29.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.63.149	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.78.24.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.255	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.179.21.194	Israel	147.237.77.212	e.dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.132.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
109.253.219.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
176.13.9.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
156.211.211.135		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
197.52.215.134	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
79.183.108.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
197.52.251.147	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
37.142.64.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.173.236.56	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
79.179.15.129	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch	Block	3
83.130.108.203	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	3
2.54.185.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.168.66.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	2
176.13.0.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.29.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.8.204.1	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakhal.idf.il/1119-he/nakhal.aspx	Block	2
156.210.57.57		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.121.15.2	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
85.64.168.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
156.210.69.19		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.147.142	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
183.206.164.12	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/admin/fckeditor/editor/	Block	1
66.249.74.75	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	1
62.210.254.52	France	147.237.72.166	aka.idf.il	Unknown Parameter amp;w in www.aka.idf.il/main/giyus/captcha.ashx	None	1
207.46.13.105	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
149.50.24.10	United States	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
87.70.2.150	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.219	Israel	147.237.76.86	navy.idf.il	Malformed URL	Block	1
185.89.217.231		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
8.37.230.83	Anonymous Proxy	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
183.206.172.12	China	147.237.76.42	refuah.idf.il	Admin Blocking	Block	1
157.55.39.125	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/8/57978.pdf.2005	Block	1
66.249.66.129	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &SortDir in www.eitan.aka.idf.il/938-en/eitan.aspx	None	1
220.181.108.89	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	1
109.64.109.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.32.212.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
183.206.172.12	China	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to chinuch.aka.idf.il/admin/fckeditor/editor/	Block	1
84.109.16.181	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
68.180.230.189	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1397-en/dover.aspx	Block	1
2.53.11.142	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
183.206.164.12	China	147.237.76.86	navy.idf.il	Distributed Admin Blocking	Block	1
66.87.19.19	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.160	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1116-he/ãƒæ'ã¢â‚¬â€•ãƒâ€šã‚¦ãƒæ'ã¢â‚¬â€•ãƒâ¢â€šâ¬šã¬ã•â	Block	1
149.50.24.10	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
46.19.85.219	Israel	147.237.76.86	navy.idf.il	Unknown HTTP Request Method onId=tsdnju55dlxdhcbnx5buk155 in URL	Block	1
185.89.217.232		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
183.206.172.12	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/admin/fckeditor/editor/	Block	1
66.249.66.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
204.79.180.101	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1