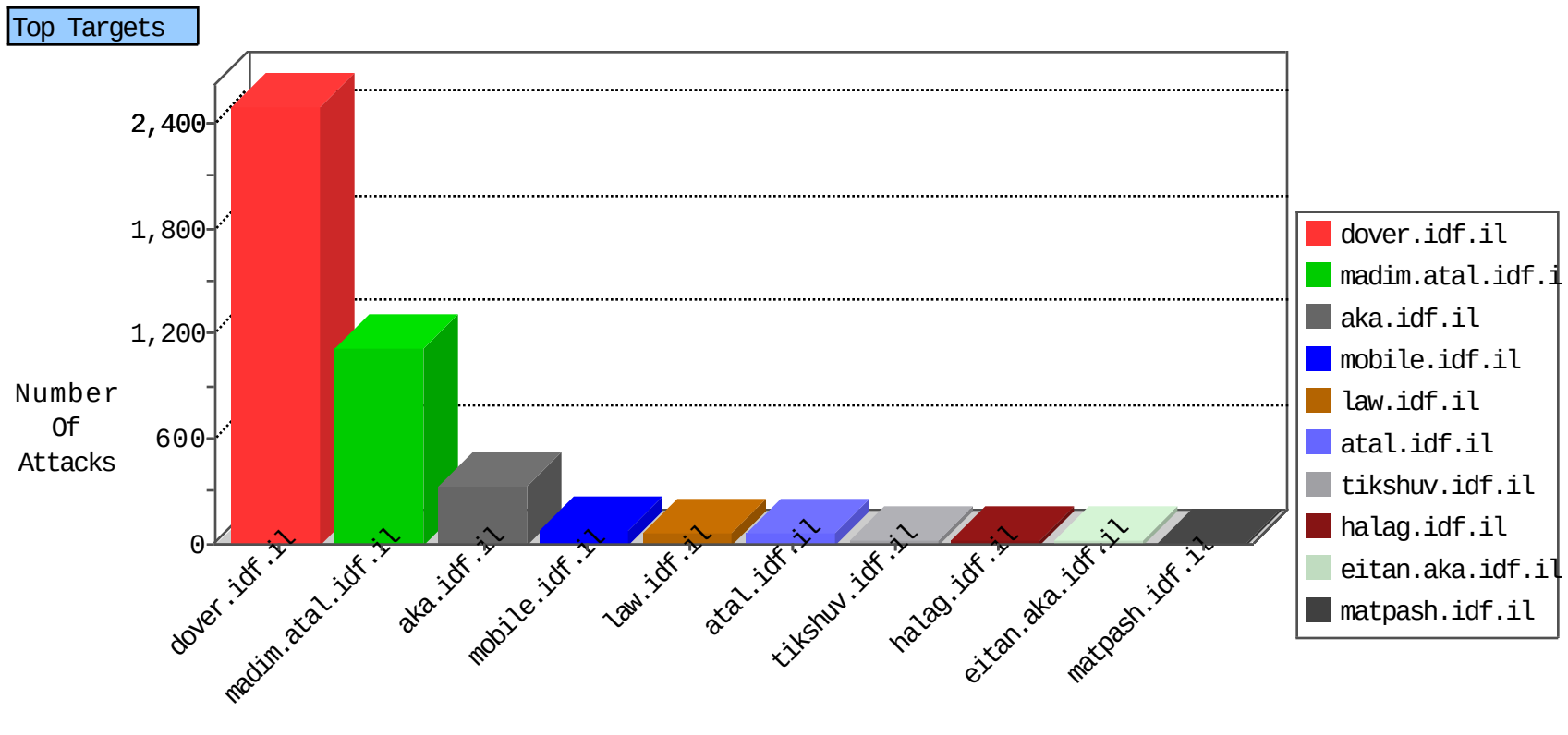
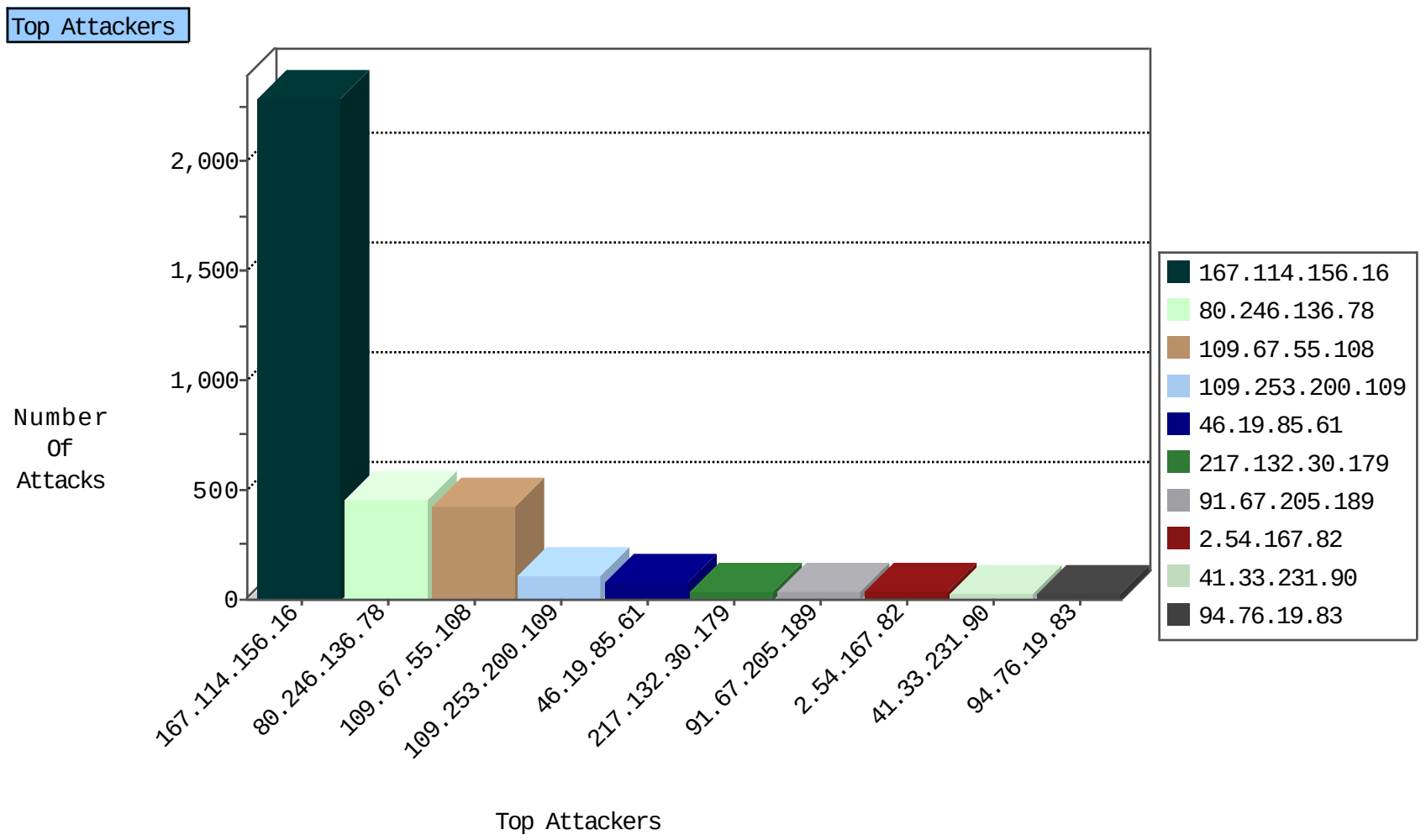
01-25-2016-23:04:06 to 01-26-2016-00:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-25-2016-23:04:06 to 01-26-2016-00:04:06

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	3146
134.191.232.69	Israel	147.237.77.233	atal.idf.il	JLM_Purple_Con_Limit_Http	drop	37
198.48.92.104	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

01-25-2016-23:04:06 to 01-26-2016-00:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-25-2016-23:04:06 to 01-26-2016-00:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.136.78	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.69.211.48	147.237.77.216	Egypt	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
94.76.2.11	147.237.0.19	Bahrain	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
89.163.148.90	147.237.77.178	Germany	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
134.191.232.69	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	1
89.163.148.90	147.237.76.39	Germany	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
113.234.218.57	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.163.148.90	147.237.72.167	Germany	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
109.235.254.181	147.237.77.121	Turkey	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
101.2.168.215	147.237.8.45	Australia	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
36.77.151.211	147.237.77.61	Indonesia	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
94.76.14.33	147.237.77.61	Bahrain	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
94.76.10.182	147.237.0.19	Bahrain	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
94.76.2.11	147.237.72.14	Bahrain	dover.idf.il(old)	ET SCAN Potential VNC Scan 5800-5820	1
191.240.136.5	147.237.77.243	Brazil	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
89.163.148.90	147.237.77.227	Germany	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
89.163.148.90	147.237.77.176	Germany	matpash.idf.il	ET SCAN Potential SSH Scan	1
116.124.223.15	147.237.8.28	Korea, Republic of	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.163.148.90	147.237.76.34	Germany	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
113.207.36.253	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
89.163.148.90	147.237.72.167	Germany	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
106.5.86.241	147.237.77.19	China	law-forum.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
101.2.168.215	147.237.8.45	Australia	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
94.76.14.33	147.237.72.14	Bahrain	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
94.76.3.158	147.237.0.33	Bahrain	idf.il	ET SCAN NMAP -sS window 1024	1

01-25-2016-23:04:06 to 01-26-2016-00:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
91.67.205.189	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
79.176.186.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.54.6.204	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
79.182.188.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.54.167.82	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
87.69.145.114	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
2.54.44.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.179.117.149	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
217.132.30.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	12
92.17.200.174	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
79.180.203.207	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
94.76.19.83	Bahrain	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	10
94.76.19.83	Bahrain	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	10
94.76.19.83	Bahrain	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	10
2.54.26.226	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
62.0.75.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
91.200.12.136	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	8
176.13.7.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.142.64.114	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.23.237	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.182.33.41	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.204.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
217.132.30.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
213.8.204.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
217.132.30.179	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.216.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
217.132.30.179	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
89.138.169.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.33.41	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.46.38.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.30.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.167.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
176.13.11.162	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.167.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.11.162	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.167.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
46.19.85.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.210.188.110	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.168.197.195	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	4

01-25-2016-23:04:06 to 01-26-2016-00:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.55.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	259
80.246.136.78	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	241
80.246.136.78	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	123
109.67.55.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	122
109.253.200.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	105
80.246.136.78	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 80.246.136.78	Block	88
46.19.85.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	71
109.67.55.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	34
46.210.181.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
5.29.245.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	17
109.64.211.141	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
46.19.85.61	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.61	Block	5
2.54.6.204	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
2.52.34.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.136.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.176.51.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.44.208	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
77.125.92.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.125.92.219	Block	2
87.69.232.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.102.254.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.7.185	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.108.97.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.19.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.29.156.60	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.185	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/misrot.aspx	Block	1
66.249.66.64	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/1/112421.pdf	Block	1
46.19.86.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.33.41	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
36.63.29.131	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1497-en/dover.	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1129-he/kkkkkkk=79615652kkkkkkk_79615652	Block	1
5.28.161.85	Israel	147.237.72.166	aka.idf.il	Illegal Parameter Encoding ctl00$ctl00$cphMain$TochenPlaceHolder$atudaControl$secondAtudaControl$ctl00d in www.aka.idf.il/main/giyus/atuda/atuda.aspx	None	1
123.125.71.43	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
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.60.4.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
80.246.136.23	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.125.92.219	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	1
176.13.3.188	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
66.249.66.67	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/1/111171.pdf	Block	1
80.246.136.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.182.49.127	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 79.182.49.127 (Unknown SSL Session)	None	1
37.26.148.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/1/size220x0/16981.jpg	Block	1
5.28.161.85	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Parameter Encoding from 5.28.161.85	None	1
149.78.227.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.231.40	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	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
46.19.85.61	Israel	147.237.0.19	madim.atal.idf.i	Too Many 404: Response Code per Session	Block	1
77.127.193.95	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1

01-25-2016-23:04:06 to 01-26-2016-00:04:06