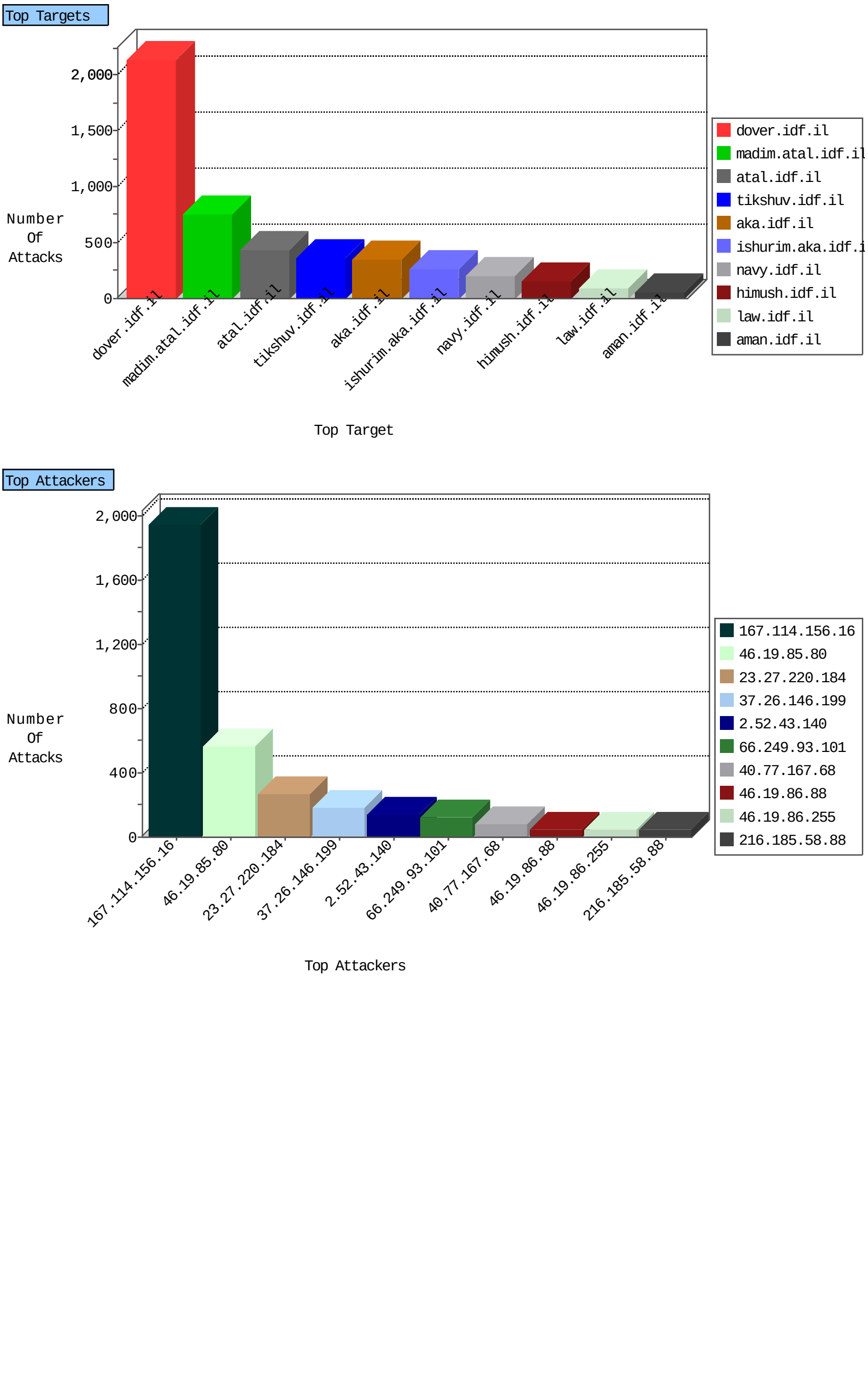
01-12-2016-11:04:01 to 01-12-2016-12:04:01

IDF Under Attack
Daily Report



01-12-2016-11:04:01 to 01-12-2016-12:04:01

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	3328
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
109.65.171.87	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
110.184.55.245	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	3
58.219.66.68	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	3
39.180.43.109	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	2
125.92.205.223	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	2
117.95.222.173	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	2
183.32.235.17	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
222.178.10.254	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
118.112.163.181	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
60.241.170.236	Australia	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
183.206.201.213	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
222.181.165.60	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
66.75.248.66	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.149	Switzerland	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
110.185.216.93	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
81.214.136.231	Turkey	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
60.166.164.251	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

01-12-2016-11:04:01 to 01-12-2016-12:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.61.83	Israel	147.237.72.167	ishurim.aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

01-12-2016-11:04:01 to 01-12-2016-12:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.101	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	125
79.177.219.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.0.102.190	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.169.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.243	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.117.9.26	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
158.255.6.220	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
109.235.254.181	147.237.76.38	Turkey	e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
93.172.239.184	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.167.162	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.13	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
185.106.92.112	147.237.8.14		e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
147.236.32.92	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.235.254.181	147.237.76.38	Turkey	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.162	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	1

01-12-2016-11:04:01 to 01-12-2016-12:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
23.27.220.184	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	271
37.26.146.199	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	182
40.77.167.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	79
46.19.86.88	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
216.185.58.88	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	44
46.19.86.255	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.85.76	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	30
185.89.217.231		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	25
185.89.217.228		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	24
185.89.217.233		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	23
185.89.217.235		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	22
46.19.85.4	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	21
46.19.85.46	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	20
185.89.217.232		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	20
213.57.194.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
185.89.217.234		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	20
185.89.217.230		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	20
109.65.102.35	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
185.89.217.225		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	18
185.89.217.231		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	17
46.19.86.246	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	17
185.89.217.233		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	16
185.89.217.227		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	16
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
185.89.217.228		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	16
185.89.217.226		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	16
185.89.217.226		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	15
185.89.217.224		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	14
185.89.217.235		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	14
185.89.217.229		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	14
185.89.217.232		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	14
185.89.217.234		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	13
185.89.217.230		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	13
84.228.32.209	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.136.111	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.66	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.80.146.93	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.89.217.229		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	11
46.19.85.156	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11
2.54.43.253	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
185.89.217.225		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
79.181.172.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.80	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.139.81	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
31.154.5.181	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
31.168.138.172	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.86.182	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
1.132.97.57	Australia	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
185.89.217.227		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	298
46.19.85.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	204
2.52.43.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	141
46.19.85.80	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.85.80	Block	52
46.210.139.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
199.203.215.1	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
109.253.130.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
83.220.54.34	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 83.220.54.34	Block	6
109.253.221.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
79.181.172.117	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	4
2.52.43.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
46.19.85.181	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
212.179.21.194	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
46.19.86.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
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	2
192.114.23.211	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
109.253.145.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.217.196	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
77.38.32.182	Slovenia	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
31.168.138.172	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.86.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.10	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/sachar/klali.aspx	None	1
2.54.23.186	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.74.31	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
80.246.137.72	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.246.137.72	Block	1
46.19.85.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.89.217.233		147.237.76.86	navy.idf.il	URL is Above Root Directory www.navy.idf.il/../images/shared/home.png	Block	1
40.77.167.62	United States	147.237.72.166	aka.idf.il	Abnormally Long Request URL	Block	1
176.10.104.243	Switzerland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	1
2.54.176.98	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.171.87	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$employmentStatesMonth in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
83.244.91.184	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
185.32.179.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.38.32.182	Slovenia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
37.26.146.199	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
132.72.10.120	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
2.54.32.112	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.117.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.230	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
207.232.46.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.137.72	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/70580.pd	Block	1
46.19.86.51	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
185.89.217.235		147.237.77.233	atal.idf.il	URL is Above Root Directory www.atal.idf.il/../images/shared/ie.gif	Block	1
46.19.85.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.15.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.224.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.185.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1