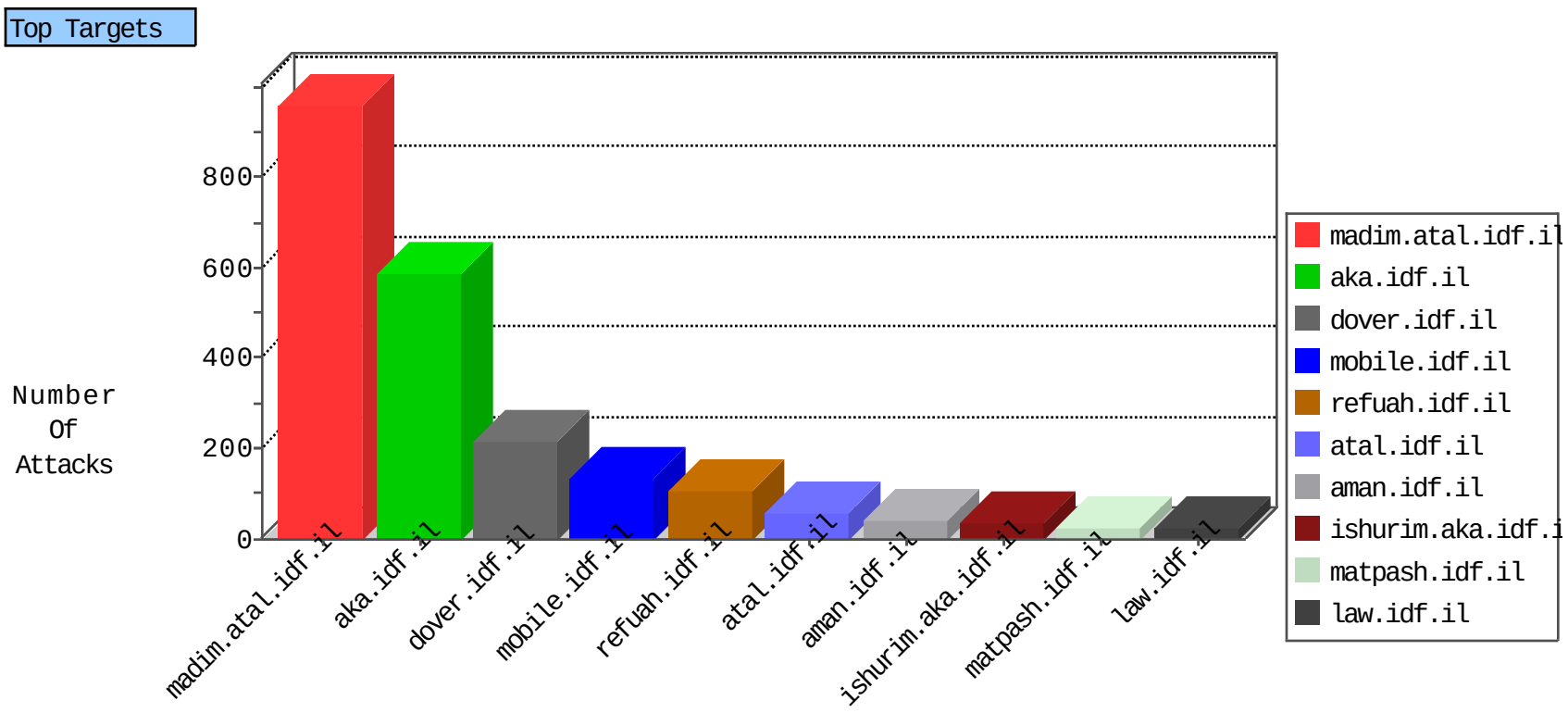
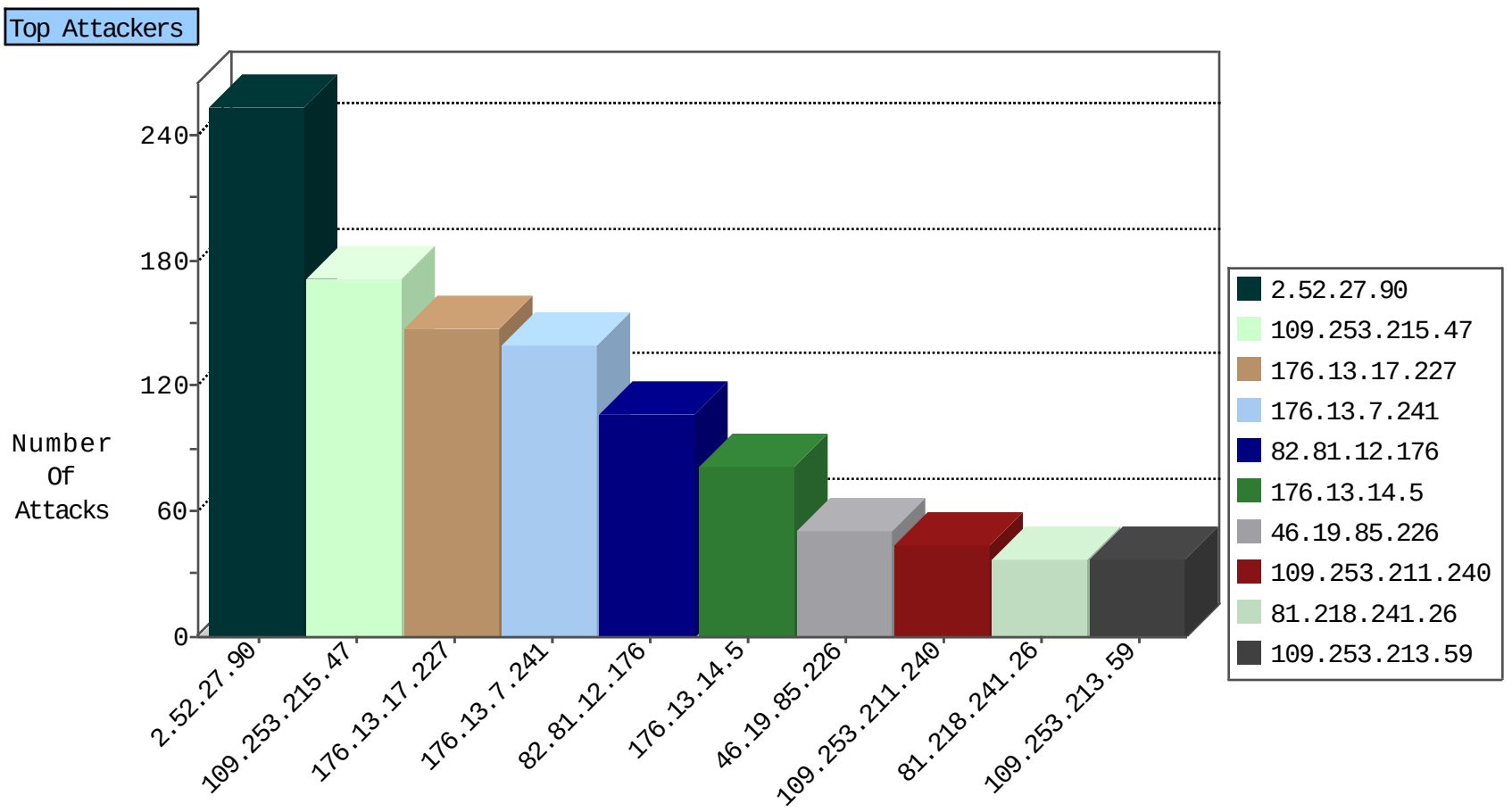
01-31-2016-09:04:01 to 01-31-2016-10:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-31-2016-09:04:01 to 01-31-2016-10:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	107
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
79.179.119.244	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
74.91.28.58	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	drop	1

01-31-2016-09:04:01 to 01-31-2016-10:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-31-2016-09:04:01 to 01-31-2016-10:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.22	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
84.110.37.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.255.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.102.7.129	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	1
46.120.144.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.55.236.147	147.237.76.31		nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.149.222	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.173.254.121	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.203.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.47.34	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
45.55.236.147	147.237.76.39		mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
37.142.153.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.130.212	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
98.119.105.221	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1

01-31-2016-09:04:01 to 01-31-2016-10:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
109.253.211.240	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
46.19.85.243	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	23
109.253.211.240	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	21
2.54.47.179	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
109.253.213.108	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
109.253.146.190	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
80.246.136.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.52.158.213	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.192.79	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.255	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.0.200.162	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.19	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.19	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
141.0.15.35	Europe	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	10
46.117.247.156	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
109.253.132.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
81.218.241.26	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.19	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.253.216.99	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
194.90.217.145	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.19	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
176.13.20.96	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
31.168.89.105	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
82.205.14.66	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.87	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.65.14	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.210.236.81	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
176.13.10.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.205.14.66	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.87	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.18.127	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.30.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.179.10.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.89.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
82.80.179.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.32.104	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.86	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.178.101.40	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.198	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
149.88.180.109	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
80.178.201.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.198	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.25	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.27.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	157
109.253.215.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	106
176.13.7.241	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	102
176.13.17.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	101
2.52.27.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	97
46.19.85.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	51
176.13.17.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	47
176.13.14.5	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	46
176.13.7.241	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	37
109.253.159.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	35
109.253.213.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	34
109.253.215.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	33
176.13.14.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
109.253.215.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	13
109.253.215.47	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 109.253.215.47	Block	11
46.19.85.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
109.253.215.47	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.215.47	Block	9
176.13.0.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
176.13.16.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
176.13.14.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	6
2.54.141.133	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	5
176.13.12.152	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
85.250.87.36	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	5
46.19.85.92	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
109.253.213.108	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
109.253.159.72	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.52.158.213	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
5.22.134.217	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	3
109.253.132.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.223.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.8.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
213.57.49.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.128.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.10.85	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.22.134.217	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 5.22.134.217	Block	2
109.253.216.177	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.177.16.23	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.143.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
194.90.240.21	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	2
81.218.140.160	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	2
176.13.9.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.192.79	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
80.246.136.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
216.72.40.185	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/login.aspx	None	1
66.249.78.154	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/back.png	Block	1
109.253.146.190	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 109.253.146.190	Block	1
2.54.139.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1