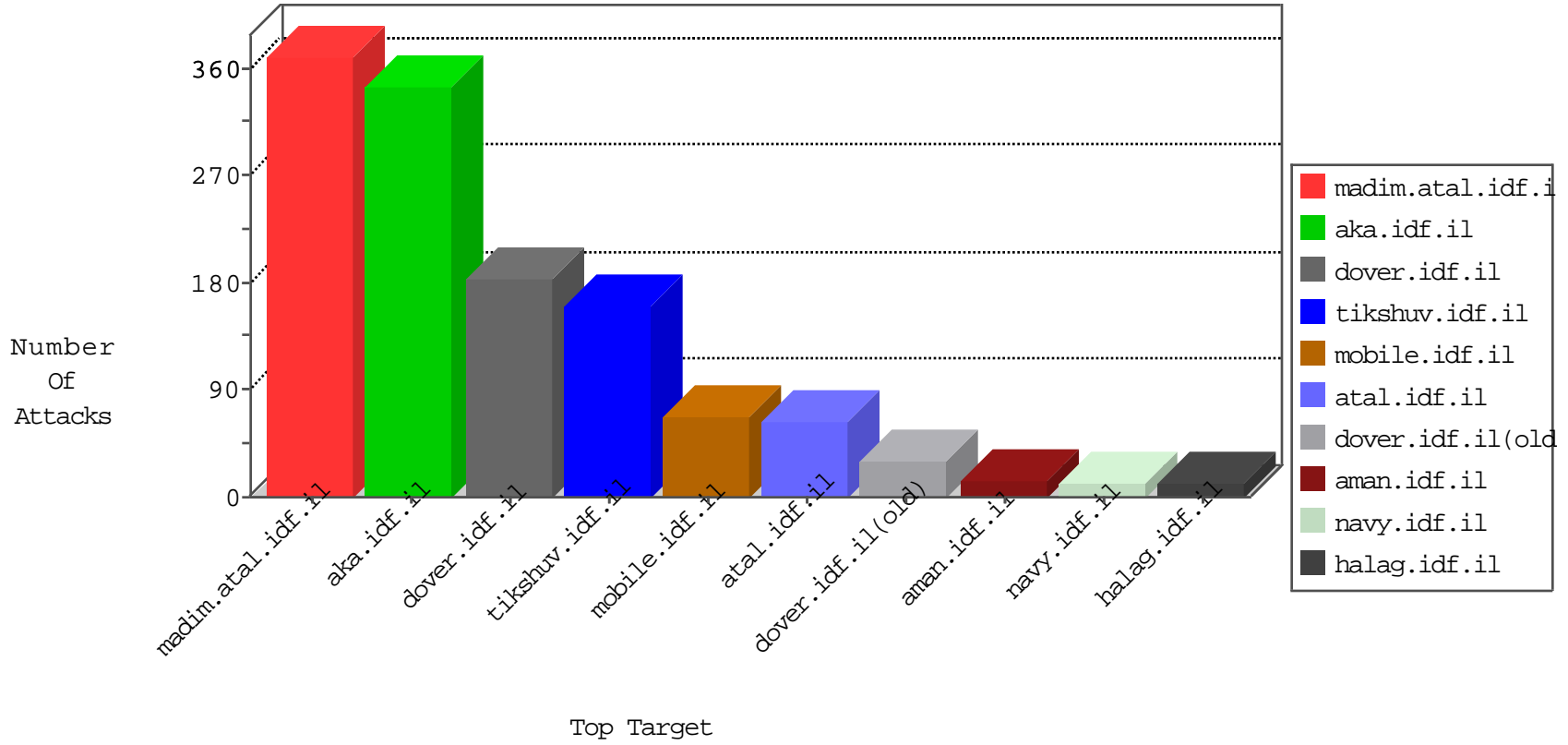


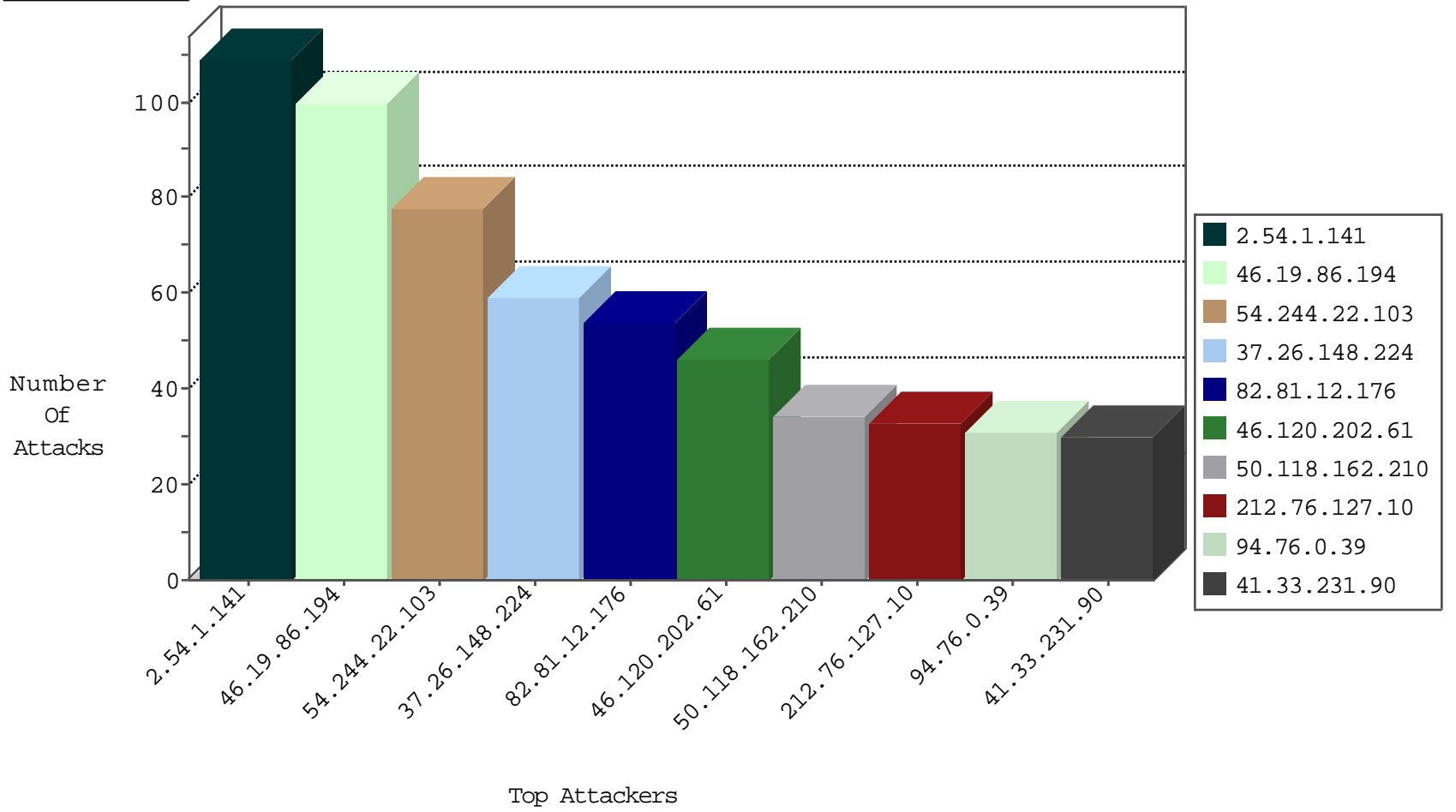
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	54
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	1

01-28-2016-20:04:08 to 01-28-2016-21:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.127	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.78.153	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
219.146.12.120	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
94.76.0.39	147.237.72.14	Bahrain	dover.idf.il(old)	ET SCAN Potential VNC Scan 5800-5820	1
219.146.12.120	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
84.228.141.9	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
219.146.12.120	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
78.219.216.138	147.237.77.179	France	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
219.146.12.120	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
219.146.12.120	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
199.180.114.67	147.237.76.39	Poland	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.162	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
219.146.12.120	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
107.182.27.36	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
219.146.12.120	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
94.76.0.39	147.237.72.14	Bahrain	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
219.146.12.120	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
79.180.115.159	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
219.146.12.120	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
219.146.12.120	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
219.146.12.120	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.161	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	69
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	33
50.118.162.210	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
94.76.0.39	Bahrain	147.237.72.14	dover.idf.il(old)	drop	SAM rule	drop	29
46.19.86.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
172.56.13.152	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	26
79.179.137.82	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
89.138.108.33	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
31.154.162.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
2.54.165.237	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
77.125.130.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
31.154.162.45	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
46.19.86.133	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.126.72.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
5.102.254.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.7.131	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
89.139.11.90	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.125	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.128.224	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.222.134	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.42	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
89.138.115.18	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
89.139.243.7	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
5.22.129.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
5.22.129.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.160.237.217	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
37.26.146.241	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
31.210.186.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
31.154.162.45	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
89.138.108.33	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.194.75	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.22.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.166.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
217.132.4.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.1.141	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.193	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
149.88.21.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.155.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.65.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.59.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.224.22	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.1.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	72
46.19.86.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	61
37.26.148.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	59
46.120.202.61	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 46.120.202.61	Block	45
46.19.86.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	39
2.54.1.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	34
85.64.4.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
46.19.86.228	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.19.86.228	Block	19
109.253.138.131	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
46.19.86.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
79.176.162.27	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	8
185.120.125.5		147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
2.54.34.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
149.50.126.150	United States	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.54.183.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
176.13.12.68	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
79.180.3.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
37.142.64.16	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	3
37.142.64.16	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	3
109.65.175.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.38.41	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.32.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.94.178.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
5.102.206.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.182.175.243	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ct100\$ContentPlaceholder1\$txtLastName in madim.atal.idf.il/1088-he/meretz.aspx	Block	2
109.253.222.134	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.111.155.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.22.134.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.142.252.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
125.46.26.253	China	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
46.19.86.11	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
125.46.26.253	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/admin-ajax.php	Block	2
89.138.107.12	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
46.121.107.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.108	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/english	Block	1
77.125.143.94	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
66.249.64.53	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/1/108191.pdf	Block	1
8.37.71.95	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11661-he/cogat.aspx&usg=alkjrhgh-oygsklj715xbs3o3pgltueh4g	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.108.172.21	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.117.218.138	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.176.213.205	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/6/110476.pdf	Block	1
46.19.86.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
37.26.146.211	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.128.224	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.34	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
5.22.129.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.138.108.33	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
46.121.243.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1