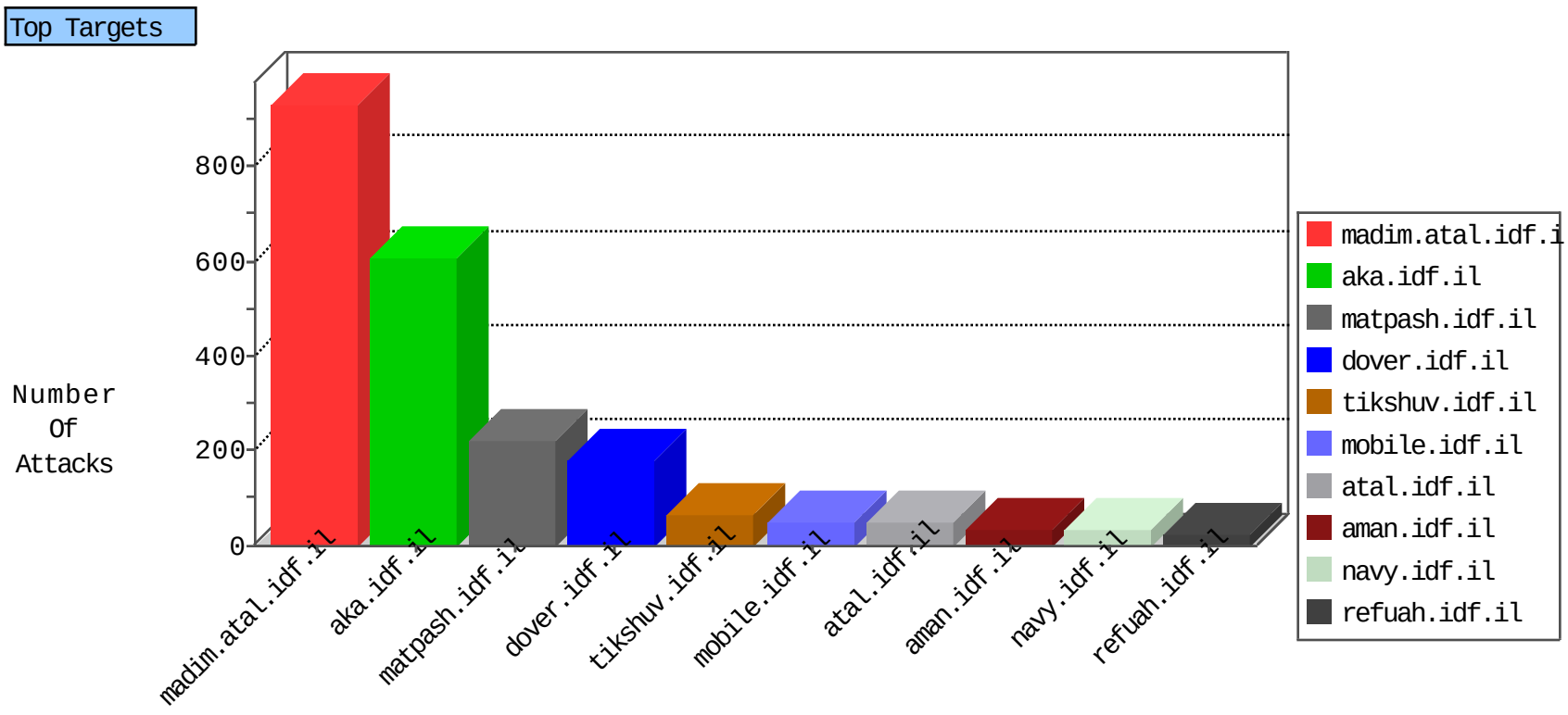
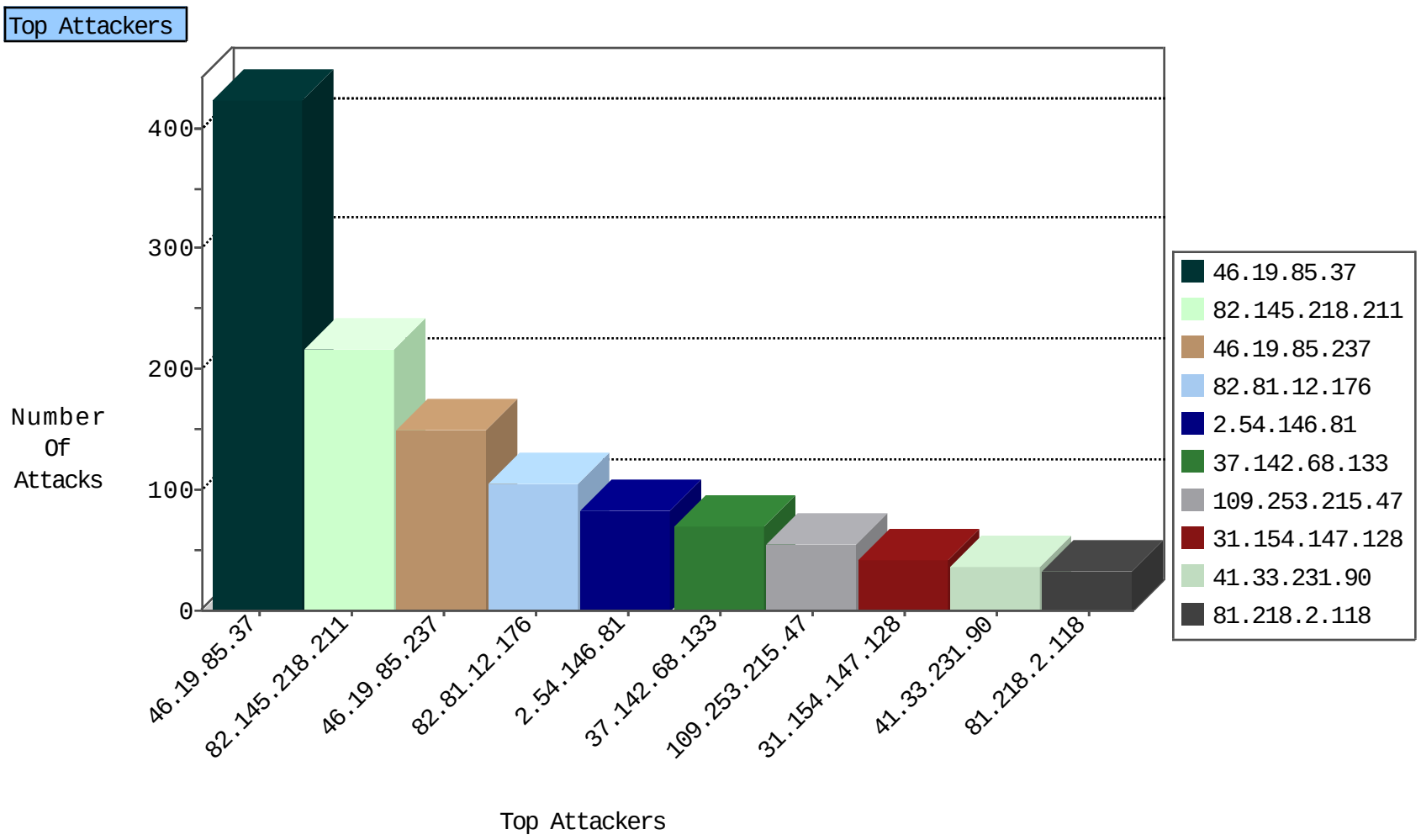
01-31-2016-08:04:09 to 01-31-2016-09:04:09

IDF Under Attack Daily Report





01-31-2016-08:04:09 to 01-31-2016-09:04:09

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	105
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
82.145.218.211	Europe	147.237.77.176	matpash.idf.il	Frk_Purple_Con_Limit_Http	drop	3
82.145.218.211	Europe	147.237.77.176	matpash.idf.il	Frk_Under_Attack_Con_Http	drop	2
74.91.28.59	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	drop	1

01-31-2016-08:04:09 to 01-31-2016-09:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-31-2016-08:04:09 to 01-31-2016-09:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.190	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
199.203.215.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.161.40.120	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
45.55.236.147	147.237.76.42		refuah.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.230.74	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.230.72	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
77.125.79.209	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.254.22	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
45.55.236.147	147.237.76.86		navy.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.230.73	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1

01-31-2016-08:04:09 to 01-31-2016-09:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.145.218.211	Europe	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	168
82.145.218.211	Europe	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
81.218.2.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
109.65.198.76	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.159	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
46.19.85.37	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
31.154.147.128	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	21
31.154.147.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
37.26.148.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
37.26.148.140	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.85.211	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
37.26.148.240	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
212.199.251.235	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
37.142.68.133	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
212.199.251.235	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
80.246.140.99	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
62.0.230.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.253.216.99	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
62.0.205.91	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	7
176.13.16.101	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.47.113	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.170.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.19.59	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
31.168.170.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.54.173.17	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.166.103.111	Israel	147.237.72.166	aka.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
176.13.6.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.200.205.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.205.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
80.246.136.87	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
109.253.216.99	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.26	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
62.90.52.101	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.26	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.154.94.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.147.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	4
37.46.39.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.109.98.89	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
2.52.158.117	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.147.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4

01-31-2016-08:04:09 to 01-31-2016-09:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	220
46.19.85.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	175
46.19.85.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	118
37.142.68.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
2.54.146.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	58
109.253.215.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	54
31.168.187.43	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 31.168.187.43	Block	31
2.52.63.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
46.19.85.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	28
213.57.49.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
2.54.136.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
2.54.146.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	19
176.13.9.57	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
109.253.213.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
176.13.0.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
2.54.43.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
2.54.171.44	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.85.37	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 46.19.85.37	Block	5
91.228.248.251	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	3
157.55.39.58	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/main/home/default.aspx	Block	3
2.54.132.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.0.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.175.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.20.24	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
194.90.15.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
188.143.232.16	Russian Federation	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 188.143.232.16	Block	2
176.13.21.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.19.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.11.215	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.147.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.4.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
91.197.103.1	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
37.48.101.193	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
2.54.154.130	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.8.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
2.54.26.43	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.143	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
46.19.86.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
181.224.157.153	Panama	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
108.61.242.65	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il./	Block	1
2.54.182.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.16.101	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.176.15.38	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
66.249.64.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/2/106582.pdf	Block	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
2.54.140.64	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.4.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.31.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-31-2016-08:04:09 to 01-31-2016-09:04:09