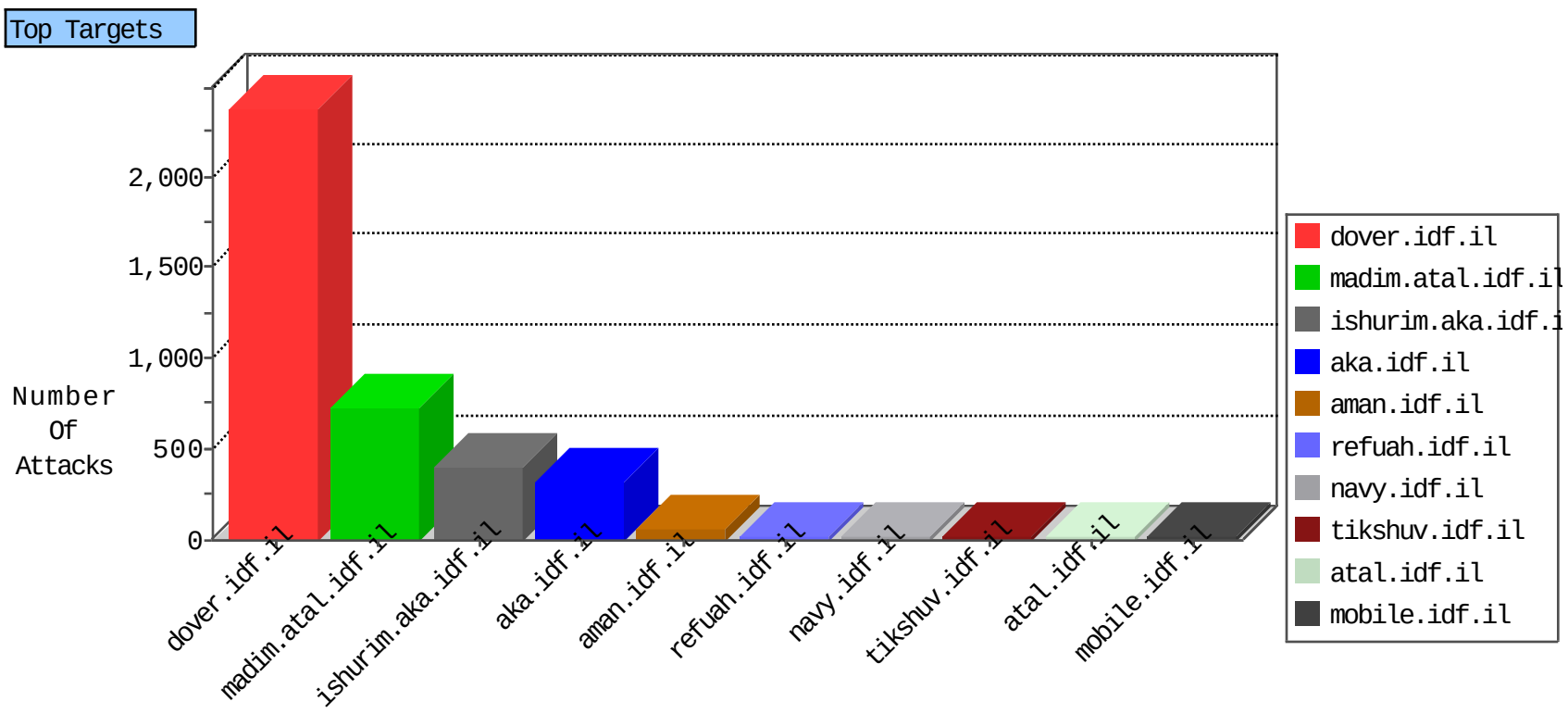
01-14-2016-10:04:01 to 01-14-2016-11:04:01

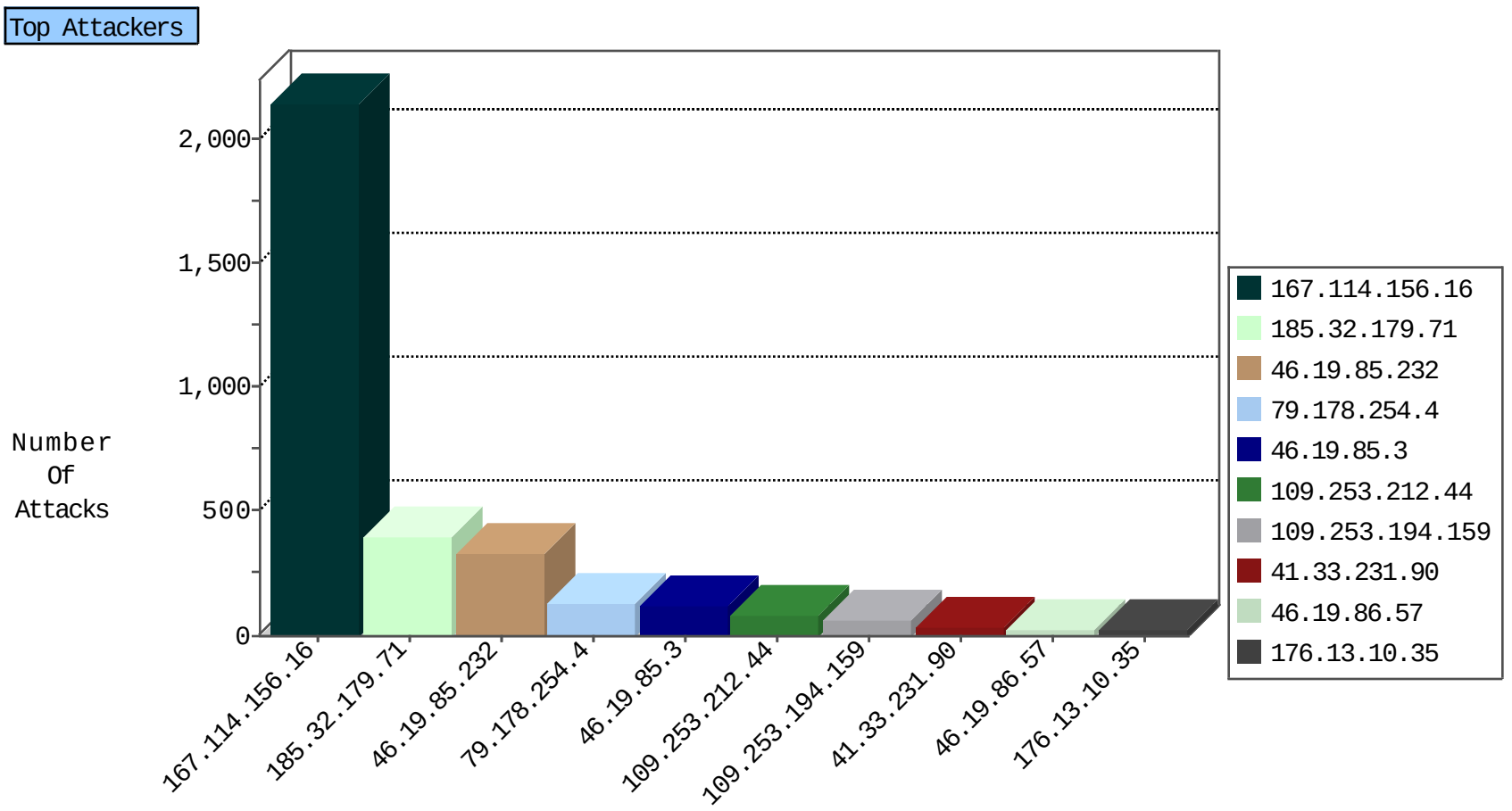
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-14-2016-10:04:01 to 01-14-2016-11:04:01

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	3190
66.249.78.2	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	28
183.12.101.186	China	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
71.6.135.131	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
183.12.101.186	China	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

01-14-2016-10:04:01 to 01-14-2016-11:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-14-2016-10:04:01 to 01-14-2016-11:04:01

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
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.23.53	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.61.149	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.91.51	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
37.26.147.135	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.215.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.77.233	Sweden	atal.idf.il	ET SCAN NMAP -sS window 1024	1
134.191.220.71	147.237.72.166	Germany	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.101.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.16	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.210.67.78	147.237.76.197	Turkey	e.himush.idf.il	ET SCAN Potential SSH Scan	1

01-14-2016-10:04:01 to 01-14-2016-11:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.232	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	335
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
79.178.254.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
79.178.254.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	26
46.19.86.57	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
79.178.254.4	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
79.178.254.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
79.178.254.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.86.154	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	14
62.0.212.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.67	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
79.178.254.4	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
79.178.132.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.67	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.114.91.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.10.36	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.142.68.80	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
2.52.154.216	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.86.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.177.0.174	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
79.178.254.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
82.80.140.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
80.246.133.204	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
62.219.137.44	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.153	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
183.79.223.155	Japan	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.179.218.166	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.198.58	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
62.0.212.169	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
2.54.145.168	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.88	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.199.251.227	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.96	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.133.204	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
213.8.204.19	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.230	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
85.130.179.174	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
62.202.184.151	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.137.229	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.178.254.4	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	4
85.130.179.174	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.118.27.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.206	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
79.178.254.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.71	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 185.32.179.71	Block	139
185.32.179.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
185.32.179.71	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 185.32.179.71	Block	85
46.19.85.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
109.253.212.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	80
185.32.179.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	64
109.253.194.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
46.19.85.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	39
176.13.10.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
109.67.251.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
2.54.175.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
185.32.179.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
217.194.195.89	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	6
176.13.11.226	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	4
217.194.195.89	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
109.253.208.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
46.19.86.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.13.178	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	2
213.57.189.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.21.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.228.129.197	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
195.130.75.82	Greece	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
80.246.136.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.146.93	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
183.79.223.155	Japan	147.237.76.200	eitan.aka.idf.il	Unknown Parameter l in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
138.134.102.16	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
49.150.200.44	Philippines	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront	Block	1
109.253.130.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.71	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
95.86.103.97	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ved in www.aka.idf.il/main/giyus/information.aspx	None	1
79.181.177.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.4.67	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.4.67	None	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
46.19.86.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
195.200.205.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
185.13.192.34	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
80.246.139.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.136.147	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
68.180.230.167	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1073-he/nakhal.aspx	Block	1
217.194.197.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	1
212.179.218.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1