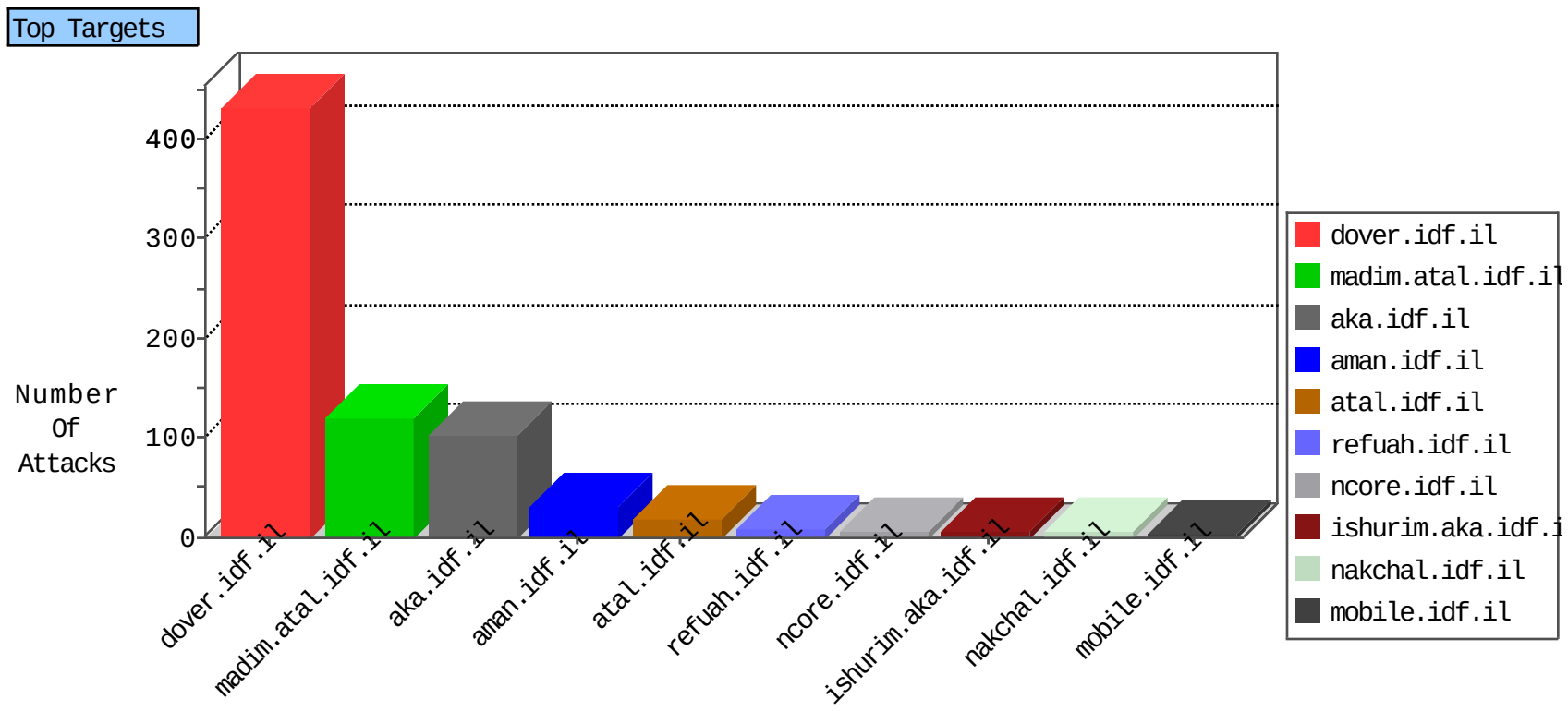
09-18-2016-07:04:01 to 09-18-2016-08:04:01

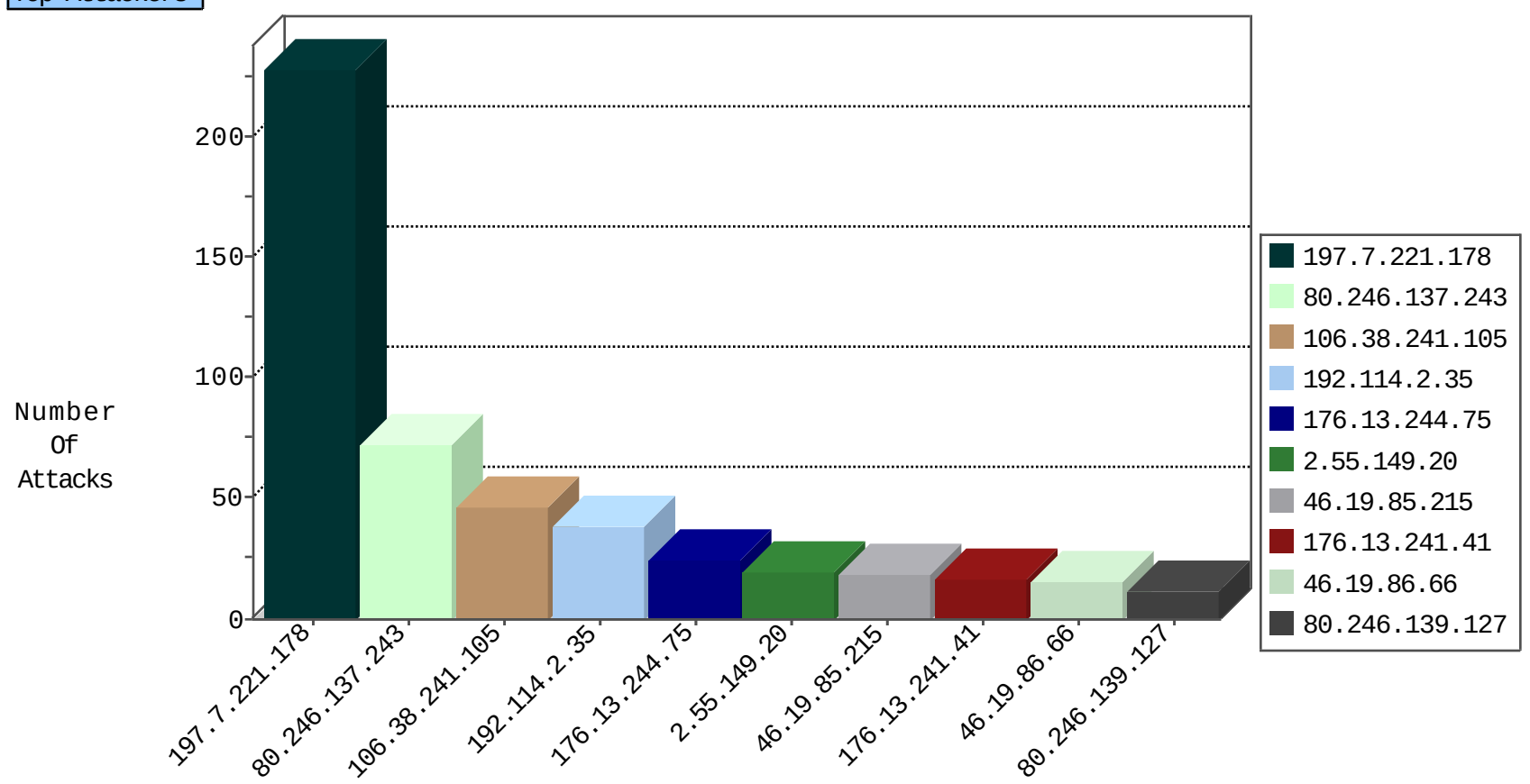
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-18-2016-07:04:01 to 09-18-2016-08:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
2.55.52.114	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
156.56.250.226	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	2
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
139.78.141.243	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
192.33.90.67	Switzerland	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	2
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.113	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	2
137.132.80.110	Singapore	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.198	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.113	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-18-2016-07:04:01 to 09-18-2016-08:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	31
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	15

09-18-2016-07:04:01 to 09-18-2016-08:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
147.236.238.22	147.237.77.216	Israel	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
213.8.204.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.129.148.230	147.237.76.34	Latvia	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.80.12	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
216.81.230.167	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
212.25.106.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.129.148.230	147.237.8.28	Latvia	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.80.12	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1
109.236.80.12	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1

09-18-2016-07:04:01 to 09-18-2016-08:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	216
192.114.2.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
176.13.241.41	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	11
2.55.149.20	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
46.19.86.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.55.149.20	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
2.53.146.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.246.139.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
82.80.196.44	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.211	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
176.13.8.209	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.215	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.26.149.211	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.215	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
80.246.130.2	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
88.202.218.233	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.32.179.102	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.112.188.72	Iraq	147.237.76.177	ncore.idf.il	drop	First packet isn't SYN	drop	3
109.253.242.121	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.211	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
109.253.150.37	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.217	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.217	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.167	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
207.46.13.15	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
80.246.133.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.145.6	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.150	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.250	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
2.53.154.169	Israel	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
46.19.86.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
80.246.138.159	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.13.17.9	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.121	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
185.112.188.72	Iraq	147.237.76.177	ncore.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	2
46.19.85.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.29	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.116.43.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
190.6.111.169	Argentina	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
2.53.164.146	Israel	147.237.77.226	www.chamatz.aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
46.19.85.125	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.102.242.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

09-18-2016-07:04:01 to 09-18-2016-08:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.137.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	72
176.13.244.75	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
37.26.149.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
77.138.43.198	France	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
79.178.200.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
82.80.170.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.181.15.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.250.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-21531-he/idfgdover.aspx	Block	1
46.19.85.215	Israel	147.237.77.233	atal.idf.il	Malformed URL	Block	1
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/templates/catalog/catalog.aspx	Block	1
114.134.189.171	Cambodia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
147.236.238.22	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
82.80.196.44	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.85.215	Israel	147.237.77.233	atal.idf.il	Multiple Abnormally Long Request from 46.19.85.215	Block	1
147.236.238.22	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
66.102.9.22	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
147.236.238.22	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method [[#21]][[#3]][[#3]][[#0]]Pê[[#18]]VKL¾å{p›³N°E	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/default.aspx	Block	1
46.19.85.215	Israel	147.237.77.233	atal.idf.il	Multiple Malformed URL from 46.19.85.215	Block	1
147.236.238.22	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method [[#21]][[#3]][[#3]][[#0]]Pê[[#18]]VKL¾å{p›³N°E	Block	1
81.218.56.171	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.56.171	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
46.19.85.215	Israel	147.237.77.233	atal.idf.il	Abnormally Long Request method	Block	1
87.69.37.129	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.179.16.219	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
46.19.85.215	Israel	147.237.77.233	atal.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.215	Block	1
147.236.238.22	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
46.19.85.215	Israel	147.237.77.233	atal.idf.il	Illegal HTTP Version __atuvs=57de1b90292d47b4000	Block	1
89.237.96.140	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/style/1.en/960http/1.1 200 okcache-control: no-cachepragma: no-cachecontent-type: text/html	Block	1
79.179.16.219	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.179.16.219	Block	1
46.19.85.215	Israel	147.237.77.233	atal.idf.il	Unknown HTTP Request Method iaimace3djbsxj45 in URL	Block	1
147.236.238.22	Israel	147.237.77.216	dover.idf.il	NULL Character in Method [[#21]][[#3]][[#3]][[#0]]Pê[[#18]]VKL¾å{p›³N°E	Block	1
82.80.170.35	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1

09-18-2016-07:04:01 to 09-18-2016-08:04:01