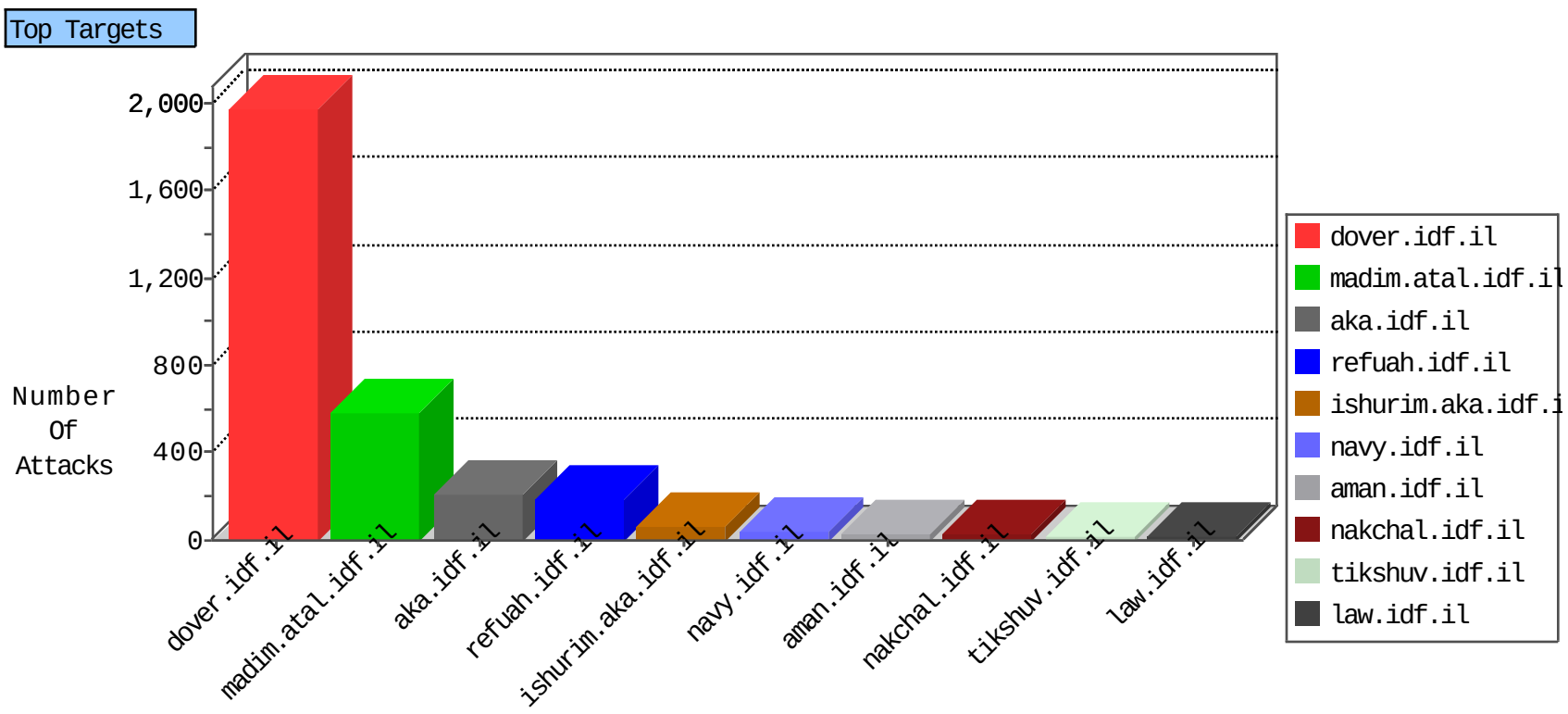
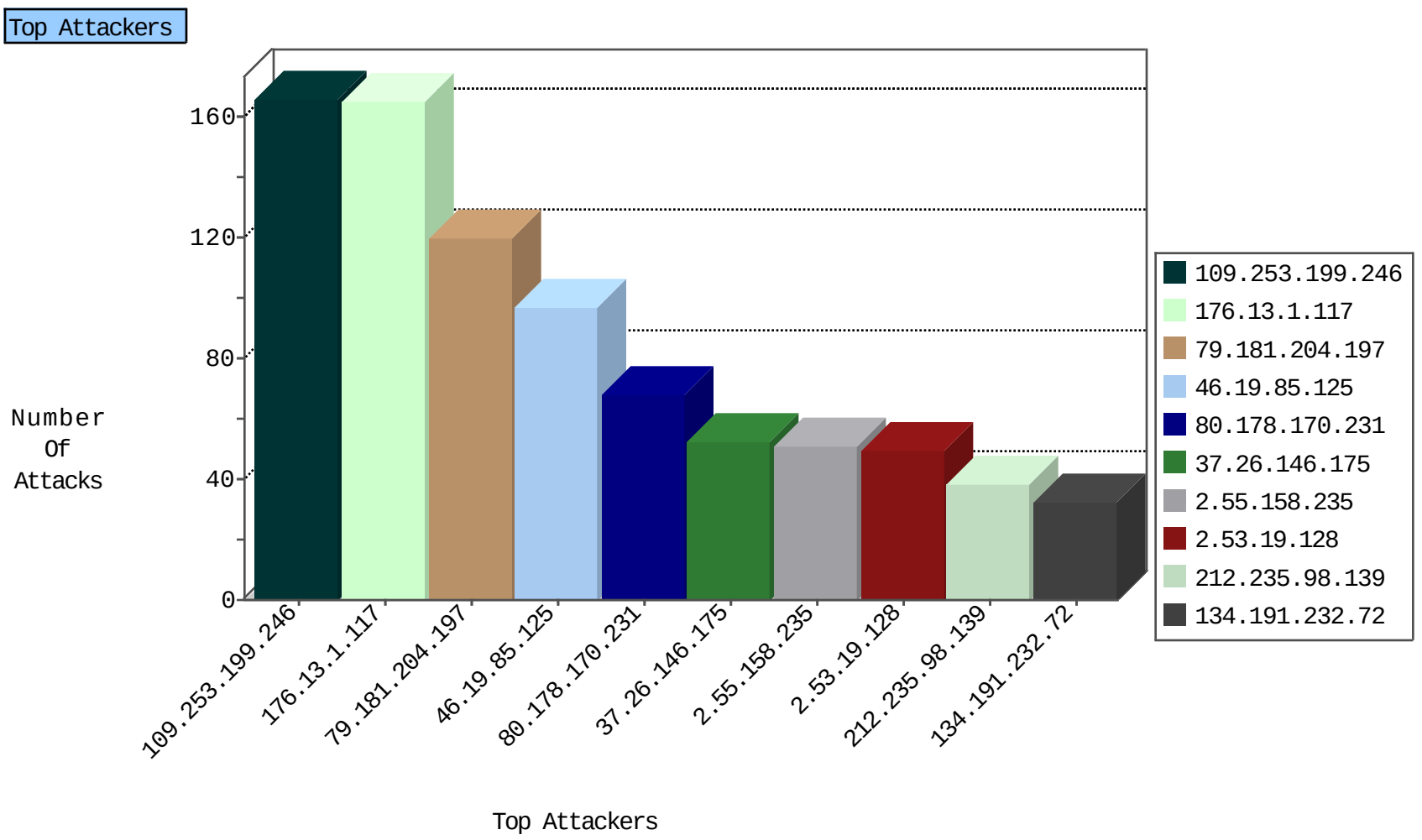
09-19-2016-14:04:02 to 09-19-2016-15:04:02

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-19-2016-14:04:02 to 09-19-2016-15:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.191.232.72	Israel	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	81
134.191.232.72	Israel	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Tcp	drop	31
37.26.149.167	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	13
2.55.33.32	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
2.53.171.184	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
195.62.53.168	Russian Federation	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	1
82.80.100.26	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-19-2016-14:04:02 to 09-19-2016-15:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
240.0.10.13		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	4

09-19-2016-14:04:02 to 09-19-2016-15:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.86.200	147.237.76.42	Israel	refuah.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	7
163.172.129.15	147.237.77.233	United Kingdom	atal.idf.il	ET SCAN NMAP -sS window 1024	1
137.74.174.250	147.237.0.19	Hong Kong	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
123.100.170.234	147.237.0.16	Korea, Republic of	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.67.207.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.237.113.239	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.23.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.23.188	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.63.84	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
72.25.36.237	147.237.72.166	United States	aka.idf.il	ET WEB_SERVER Poison Null Byte	1
163.172.129.15	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.229.111	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
137.74.174.250	147.237.0.35	Hong Kong	akaws.idf.il	ET SCAN Potential SSH Scan	1
128.232.110.28	147.237.76.177	United Kingdom	ncore.idf.il	ET SCAN Potential SSH Scan	1
109.253.205.167	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.98.176.73	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.18.244	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.202.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.126.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.114.91.248	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-19-2016-14:04:02 to 09-19-2016-15:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.181.204.197	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	120
80.178.170.231	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	68
2.55.158.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
132.72.153.191	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
176.13.8.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
138.134.192.10	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	26
62.0.221.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
95.35.155.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
80.246.130.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.116.100.59	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
93.172.112.110	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
46.19.86.153	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	13
2.53.63.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
134.191.232.72	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
217.132.110.60	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
109.253.143.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.161	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
37.26.149.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
176.13.245.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
109.253.199.246	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
46.19.85.236	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.124	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.53.50.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.53.129.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
5.102.195.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.106	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
195.60.232.57	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
62.0.221.129	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	9
46.19.86.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.170.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.53.150.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
152.62.109.204	Europe	147.237.76.86	navy.idf.il	drop	SAM rule	drop	8
2.53.24.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
151.34.127.141	Italy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
109.253.200.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
77.127.43.80	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
84.229.4.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.210.206.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.148.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
156.204.16.63	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.229.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.20.168	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.255	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.147.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

09-19-2016-14:04:02 to 09-19-2016-15:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.1.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	165
109.253.199.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	154
46.19.85.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	85
37.26.146.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	52
2.53.19.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	49
2.53.37.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
109.253.214.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
46.19.85.125	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	9
77.126.89.16	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	5
109.252.29.58	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	4
176.13.228.0	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	4
176.13.241.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.4.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.129.106	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.32.179.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	3
77.126.89.16	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/5/	Block	3
109.64.141.19	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
37.142.8.32	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
5.22.134.247	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
213.57.48.97	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.86.212	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
84.94.103.219	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22448-he/idfgdover.aspx؟	Block	2
46.19.85.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.235.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
93.172.112.110	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
66.249.65.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1384-12681-he/dover.aspx	Block	1
46.19.85.168	Israel	147.237.76.86	navy.idf.il	Suspicious Response Code	Block	1
195.62.53.168	Russian Federation	147.237.76.42	refuah.idf.il	Unauthorized URL Access to gmail.com/engine/log.txt	Block	1
81.218.37.2	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/5/1475.png	Block	1
72.25.36.237	United States	147.237.72.166	aka.idf.il	Unknown HTTP Request Method q[[#0]][[#0]][[#0]][[#23]]¤VÆ‰Š6®[[#25]]áì•¿Ä[[#28]]ç in URL °' +Ý¬Ûd•5¯n©¤×x©	Block	1
138.134.102.15	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.229.223	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
84.109.10.49	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1250-he/atal.aspx	Block	1
52.30.171.229	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to /	Block	1
213.8.204.12	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
77.138.102.30	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
109.253.206.185	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
72.25.36.237	United States	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1
101.178.206.92	Australia	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/tiki/vendor_extra/elfinder/elfinder.html	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/default.asp	Block	1
207.46.13.115	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
82.81.73.109	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
77.126.89.16	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 77.126.89.16	Block	1
72.25.36.237	United States	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
85.64.26.233	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
62.0.192.63	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/miluim/templates/inner.asp	Block	1
185.32.179.46	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 185.32.179.46	Block	1
77.138.171.111	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1

09-19-2016-14:04:02 to 09-19-2016-15:04:02