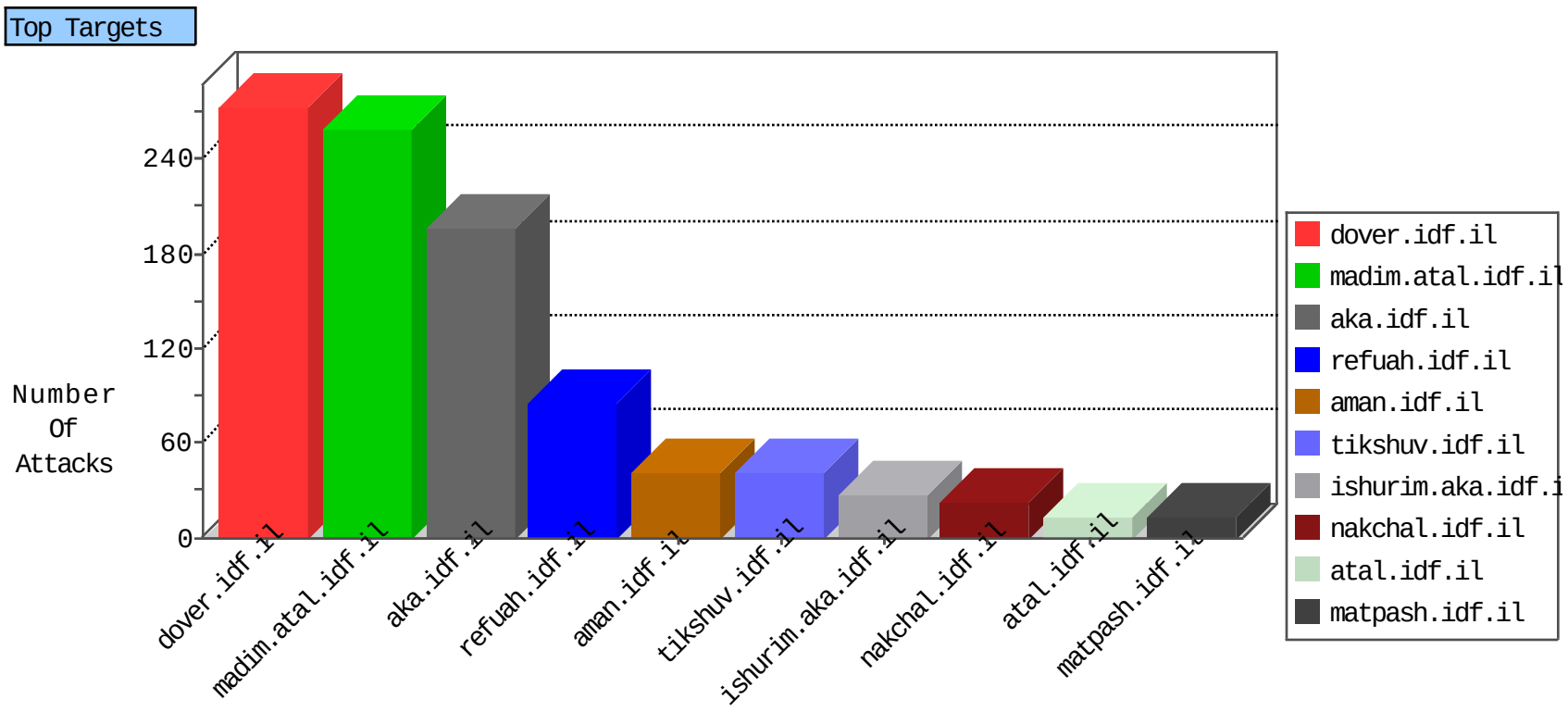
09-19-2016-13:04:06 to 09-19-2016-14:04:06

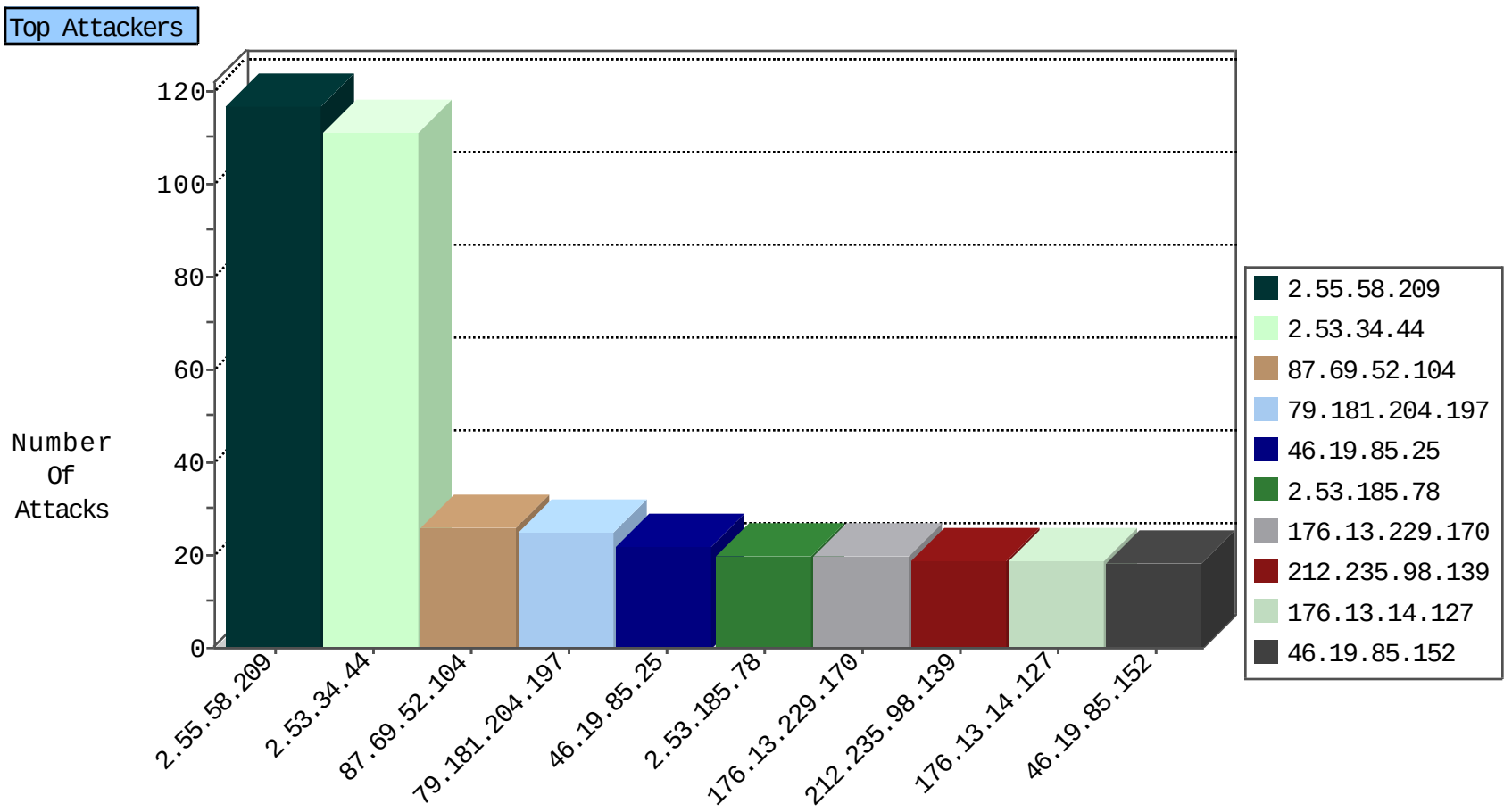
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-19-2016-13:04:06 to 09-19-2016-14:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.25.74.130	Israel	147.237.77.216	dover.idf.il	Black List	drop	12
109.253.157.117	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
212.25.74.130	Israel	147.237.72.167	ishurim.aka.idf.il	Black List	drop	6
176.13.248.239	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
31.168.240.21	Israel	147.237.72.156	aman.idf.il	Black List	drop	3
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Black List	drop	3
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.42.142.45	United States	147.237.72.166	aka.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	1
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	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
106.186.113.132	Japan	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1

09-19-2016-13:04:06 to 09-19-2016-14:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
108.59.8.70	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-19-2016-13:04:06 to 09-19-2016-14:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.0.109.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.169.70.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.208.243	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.136.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.80.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.28.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.237.124.202	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.12.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.0.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.136.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.132.30.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.55.57	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.242.184	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.135	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.72.172.153	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.195.147	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.145.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.129.80	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.102.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
88.202.218.238	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.49.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.58.131	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.102.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
216.81.230.167	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1

09-19-2016-13:04:06 to 09-19-2016-14:04:06

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	24
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
176.13.229.170	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
37.26.146.140	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	14
46.19.86.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
87.69.79.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
87.69.52.104	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
87.69.52.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
46.19.86.236	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	12
192.114.180.18	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.25	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.85.25	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.13.14.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
80.246.136.73	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
109.253.192.253	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.212.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.60	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
62.0.229.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.14.127	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.60	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.114.180.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.225	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
217.194.199.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
212.179.219.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.179.114.11	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.207	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.179.219.237	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.55.181.108	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
87.69.55.51	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.55.181.108	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
213.57.133.162	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.53.185.78	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.73	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.53.185.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.73	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
213.8.10.15	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.53.185.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.231.192.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
176.13.14.127	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.185.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.178.43.65	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.185.78	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.85.73	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.49	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4

09-19-2016-13:04:06 to 09-19-2016-14:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.58.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
2.53.34.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
175.44.17.50	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 175.44.17.50	Block	12
199.203.68.10	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	11
109.253.192.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.53.161.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
46.19.85.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
84.95.251.107	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
199.203.37.197	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
175.44.17.50	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	4
46.19.85.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.199.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.62.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.27.106.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.57.62.132	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
92.54.222.163	Georgia	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
46.19.85.152	Israel	147.237.76.31	nakchal.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.152	Block	2
217.194.199.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
81.218.97.45	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
5.29.7.71	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.85.152	Israel	147.237.76.31	nakchal.idf.il	Multiple Malformed URL from 46.19.85.152	Block	2
5.29.145.36	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
189.218.100.7	Mexico	147.237.77.235	sviva.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
176.13.249.146	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
46.19.86.105	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method 2np5uv55 in URL	Block	1
189.219.179.92	Mexico	147.237.76.31	nakchal.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
2.53.63.22	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
187.160.159.208	Mexico	147.237.0.15	kosher-kravi.idf.i	Multiple Redundant HTTP Headers in header Content-Type	Block	1
79.181.204.197	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.102.9.26	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
175.44.17.50	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
201.162.8.198	Mexico	147.237.0.19	madim.atal.idf.il	Redundant HTTP Headers Content-Type	Block	1
85.65.60.135	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
10.102.70.15		147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
189.218.146.86	Mexico	147.237.77.170	maarachot.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
178.255.87.242	United Kingdom	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/robots.txt	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Unknown HTTP Request Method þÛppzì[[#24]][[#8]]]Ä…[[#5]][[#1]]$••[[#22]]×Ø[Ál†*Ç:[[#28]]¸ßßßl·áà ü–[[#15]] in URL	Block	1
46.116.23.137	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/faq.aspx	None	1
213.127.19.49	Netherlands	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
46.19.85.152	Israel	147.237.76.31	nakchal.idf.il	Malformed URL	Block	1
101.178.206.92	Australia	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/broadweb/bwroot.asp	Block	1
188.120.148.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.61.166.51	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.64.128	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/.well-known/assetlinks.json	Block	1
176.13.2.35	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
155.145.208.131	United Kingdom	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
46.19.85.152	Israel	147.237.76.31	nakchal.idf.il	Unknown HTTP Request Method e&f=894 in URL	Block	1

09-19-2016-13:04:06 to 09-19-2016-14:04:06