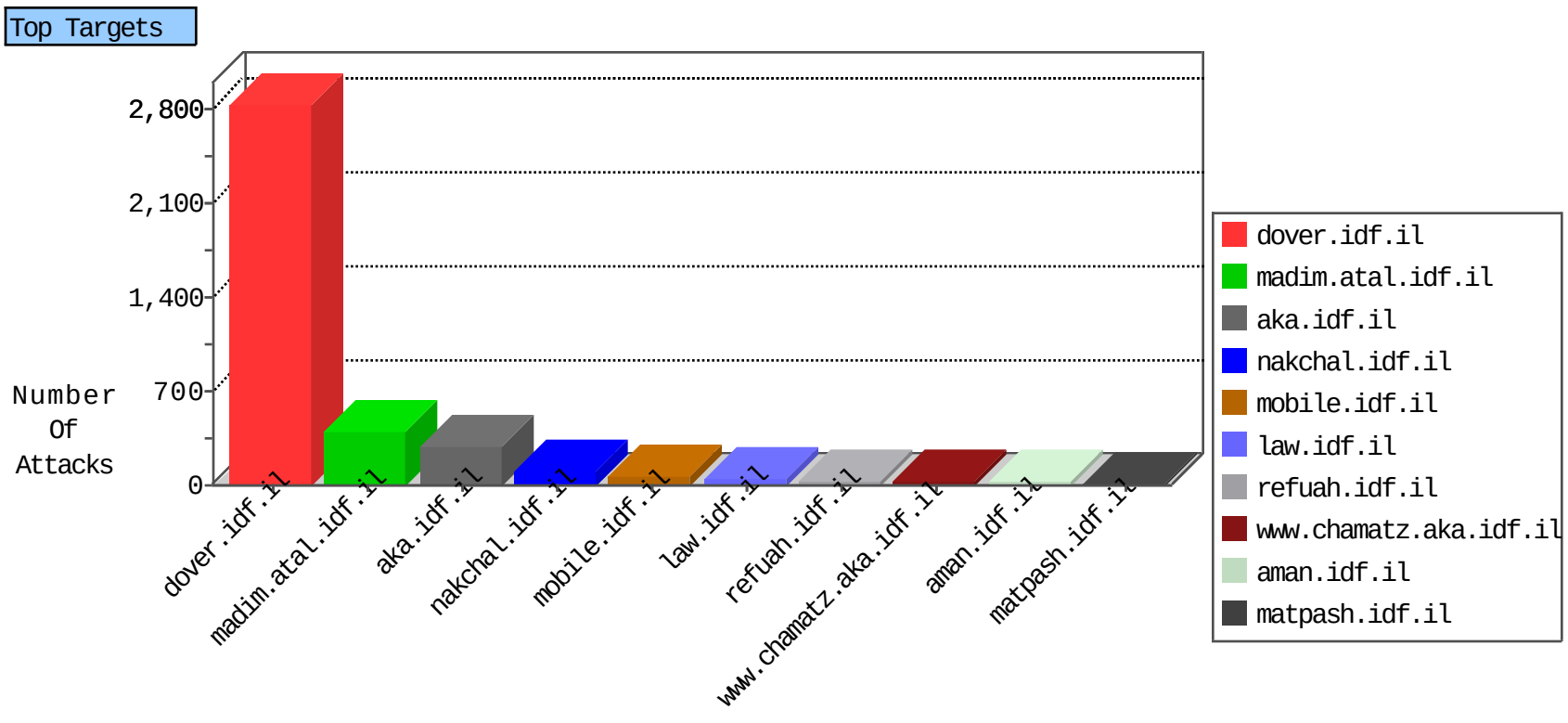
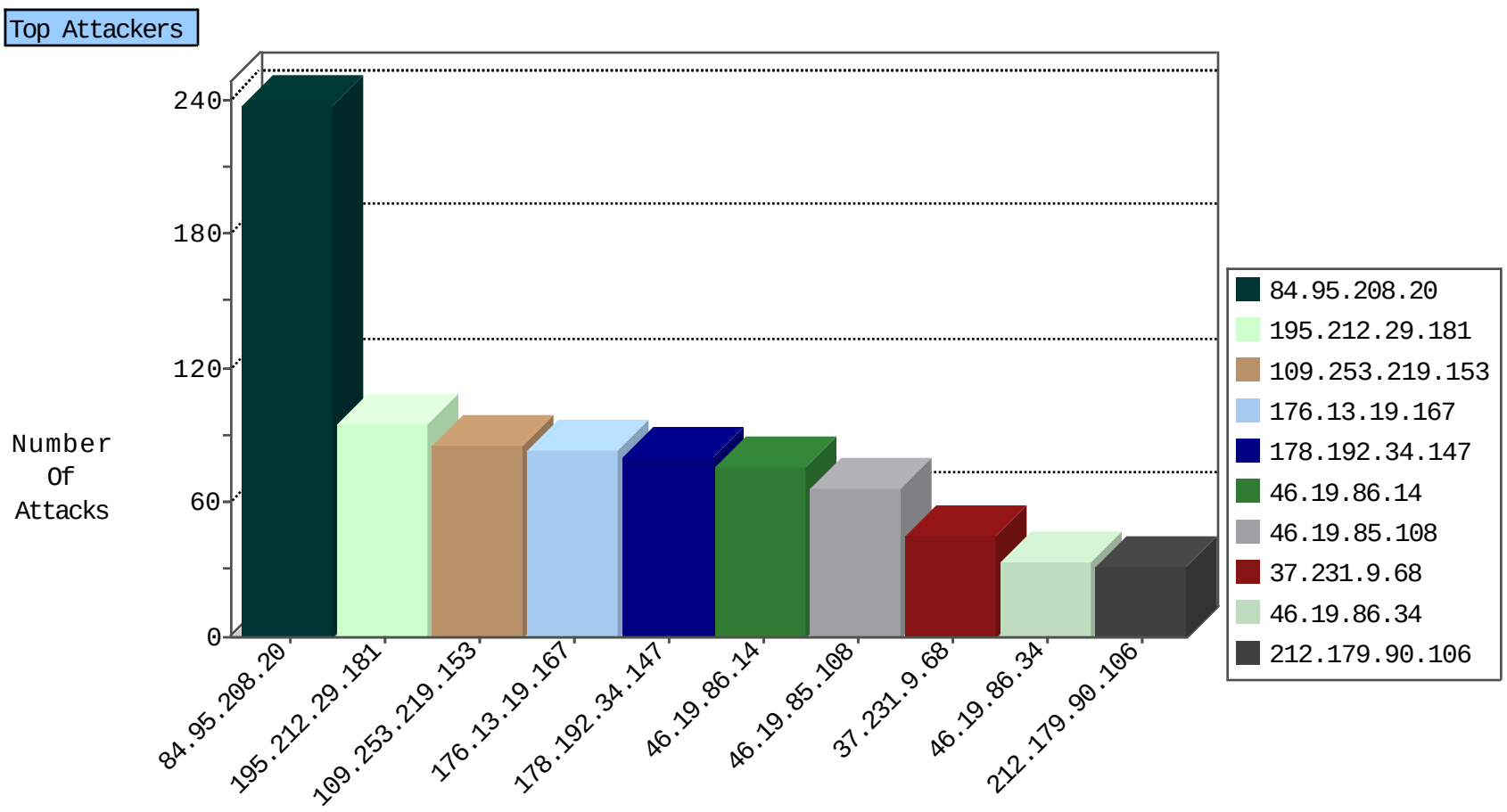
09-28-2016-11:04:07 to 09-28-2016-12:04:07

IDF Under Attack Daily Report





09-28-2016-11:04:07 to 09-28-2016-12:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.186.171	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	31
109.253.206.4	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
93.174.94.235	Netherlands	147.237.76.176	test.ncore.idf.il	Black List	drop	1
31.168.26.13	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
91.230.121.156	Ukraine	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
2.55.25.135	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
93.158.200.70	Netherlands	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1

09-28-2016-11:04:07 to 09-28-2016-12:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
163.172.220.113	United Kingdom	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
71.6.146.186	United States	147.237.77.179	e.mazi.idf.il	2226: Backdoor: TCP Window Size 55808 Trojan	Block	1
151.80.31.183	France	147.237.72.156	aman.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

09-28-2016-11:04:07 to 09-28-2016-12:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.86.254	147.237.76.31	Israel	nakchal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
58.218.200.137	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
2.53.160.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
216.72.40.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.230.71	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
185.28.155.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.160.176.212	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.155	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.155	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
62.219.196.102	147.237.77.226	Israel	www.chamatz.aka.idf.il	LOCAL_RULES - HTTP Request with OPTIONS method to a .doc file	1
2.53.12.247	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.29.202.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.120.154.7	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.129.15	147.237.0.16	United Kingdom	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
104.160.176.212	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
91.201.236.155	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
67.211.219.120	147.237.76.44	United States	e.refuah.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

09-28-2016-11:04:07 to 09-28-2016-12:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
195.212.29.181	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
37.231.9.68	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
2.53.159.3	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
62.0.210.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
46.19.86.34	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
109.253.138.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
46.19.86.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
46.19.86.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	19
109.65.173.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	17
2.53.133.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
46.19.86.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
46.19.85.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.80	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.191	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
141.226.217.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.86.213	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
212.143.144.153	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
89.139.153.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	13
176.13.2.88	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.237.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.114.23.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.34	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
159.46.196.31	Netherlands	147.237.77.216	dover.idf.il	HTTP Format Sizes	'Proxy-Authorization' header length exceeded maximum allowed length	monitor	12
46.19.86.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.86.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
194.90.66.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
62.90.94.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.36	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.118	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.26.149.213	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
193.47.165.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.116.108.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.178.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.26.146.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.55.139.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.253.156.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
159.46.196.31	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.53.182.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8

09-28-2016-11:04:07 to 09-28-2016-12:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	99
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	87
109.253.219.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
176.13.19.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
46.19.86.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
46.19.85.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
46.19.86.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	18
2.55.178.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	9
2.53.35.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
81.218.251.251	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	5
2.53.53.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
2.53.29.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
2.53.35.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
194.90.200.70	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.200.70	Block	4
81.218.251.251	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 81.218.251.251	Block	4
109.253.220.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.53.10.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.55.26.93	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	3
2.53.18.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.57.153.173	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
195.212.29.180	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	3
46.19.86.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.229.45.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	3
192.118.68.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kapatz/undefined	Block	3
88.202.218.233	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
132.72.86.150	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.86.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.138.97.76	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/forms.aspx	Block	2
212.205.110.163	Greece	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.53.19.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
199.203.151.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.67.99.70	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	2
181.48.157.156	Colombia	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
80.178.101.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
5.102.222.6	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
213.8.204.2	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/homepage/piwik.php	Block	1
194.68.142.52	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
66.249.69.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8921-he/refuah.aspx	Block	1
88.202.218.233	United Kingdom	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
212.179.224.187	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
181.48.157.156	Colombia	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 181.48.157.156	Block	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
109.67.99.70	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/7/	Block	1

09-28-2016-11:04:07 to 09-28-2016-12:04:07