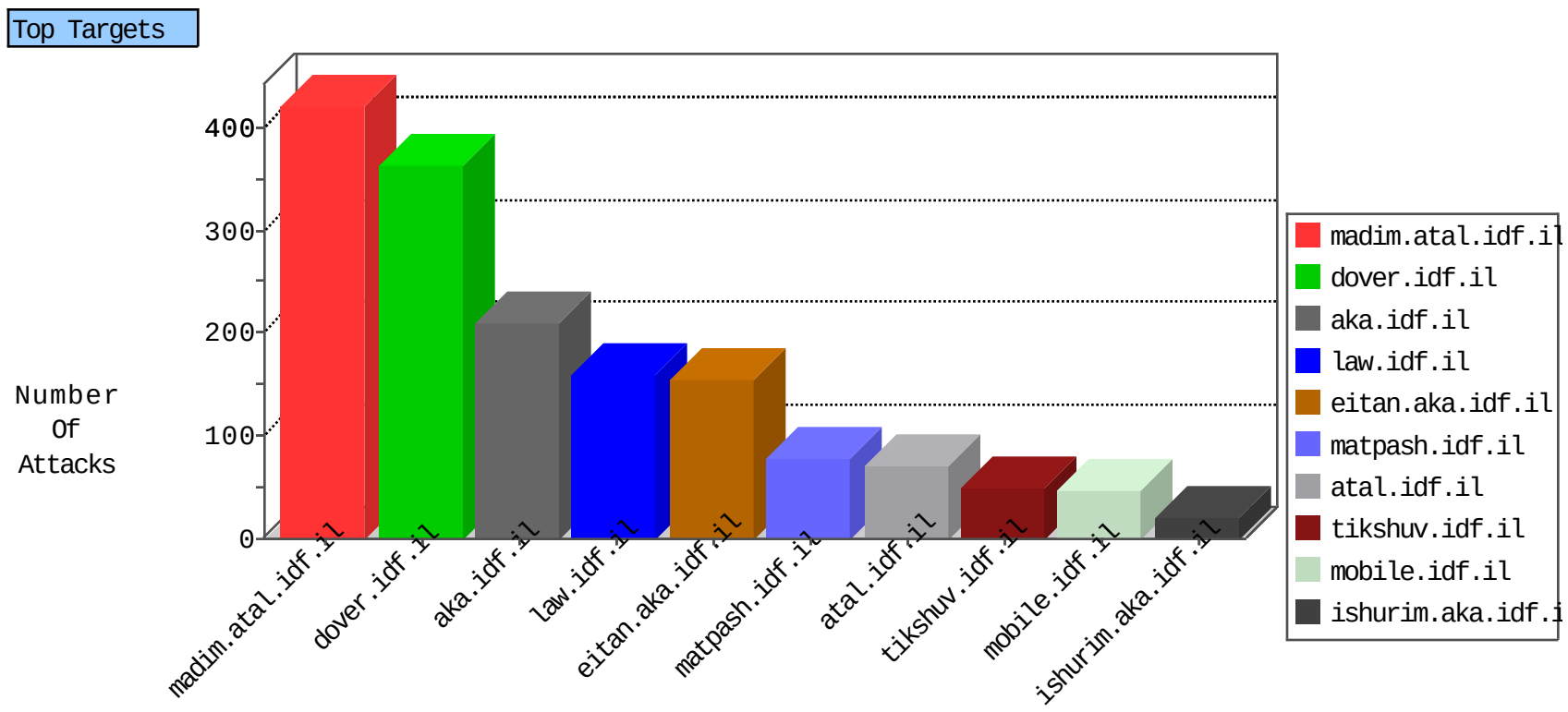
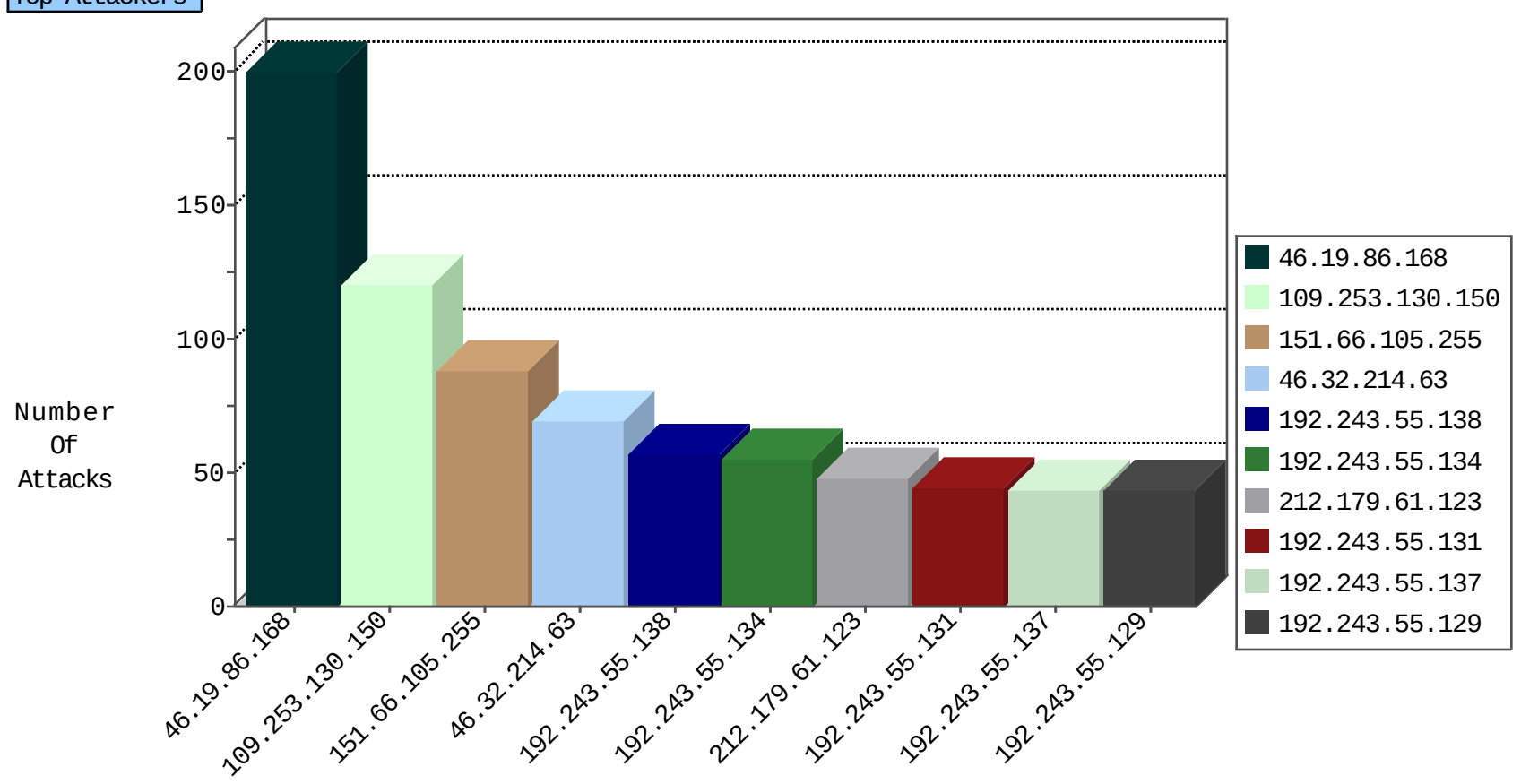
03-10-2016-12:04:07 to 03-10-2016-13:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-10-2016-12:04:07 to 03-10-2016-13:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.32.214.63	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SQL-Inj-Pang-GMSSQLInt1	dest-reset	58
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
89.248.172.207	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.97	United States	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.207	Netherlands	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.72.217	e.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.207	Netherlands	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
209.203.106.50	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.196	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1

03-10-2016-12:04:07 to 03-10-2016-13:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.166.198.189	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
2.52.149.24	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
176.13.5.251	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
176.13.14.171	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
109.64.125.21	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
192.118.12.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
46.116.28.74	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
157.55.2.154	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
207.46.13.98	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-10-2016-12:04:07 to 03-10-2016-13:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.243	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	3
80.246.133.111	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
80.74.118.148	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.198.61	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
54.183.114.72	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
212.143.99.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.228.12.4	147.237.0.17	Tunisia	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
104.197.254.53	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
31.168.215.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.189.26.18	147.237.72.14	Austria	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
2.54.7.58	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.162.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.130.89	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
79.182.135.237	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
68.180.229.239	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.195.166	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
46.32.214.63	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SQL 1 = 1 - possible sql injection attempt	1
178.62.94.12	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
41.228.12.4	147.237.0.17	Tunisia	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
104.197.254.53	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -f -sS	1
5.29.99.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.192.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.142.143	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

03-10-2016-12:04:07 to 03-10-2016-13:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
151.66.105.255	Italy	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	88
212.179.61.123	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
109.67.110.209	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.93.67	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	15
2.52.44.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.25.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.17.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
81.218.192.106	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
62.0.252.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.32.214.63	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.117.81.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
80.246.133.111	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
80.246.130.89	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
80.246.133.111	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
80.246.140.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
80.246.130.89	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
31.154.249.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.134	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
62.0.252.65	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
192.115.177.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.138	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.213.121	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
147.235.8.75	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
81.218.71.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5

03-10-2016-12:04:07 to 03-10-2016-13:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	200
109.253.130.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	120
2.54.24.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
109.253.219.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
2.54.24.35	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	9
46.19.85.9	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	5
2.54.52.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
157.55.2.159	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
2.54.128.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.146.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.8.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
213.57.231.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.25.2	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.118.118.126	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
31.168.116.1	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 31.168.116.1	Block	2
62.90.77.54	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	2
188.161.153.68	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx	Block	2
109.253.220.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.115.90.66	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 192.115.90.66	Block	2
46.117.81.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
46.118.118.126	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.118.118.126	Block	2
45.79.89.188		147.237.72.167	ishurim.aka.idf.i	NULL Character in Header Name at [[#0]]4[[#0]]2[[#0]][[#14]][[#0]]#012[[#0]][[#25]][[#0]][[#11]][[#0]][[#12]][[#0]][[#24]][[#0]]#011[[#0]]	Block	1
134.191.232.68	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.69.37.129	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
37.26.146.210	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
212.199.118.121	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.129	Dominica	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18842-en/	Block	1
149.88.161.108	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 149.88.161.108	Block	1
45.79.89.188		147.237.72.167	ishurim.aka.idf.i	Illegal Byte Code Character in Header Name [[#0]]ÿ[[#1]][[#0]][[#1]]c[[#0]][[#0]][[#0]][[#27]][[#0]][[#25]][[#0]][[#0]][[#22]]www.ishurim.aka.idf.il[[#0]][[#11]][[#0]][[#4]][[#3]][[#0]][[#1]][[#2]][[#0]]	Block	1
216.72.40.185	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	1
5.18.54.181	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
212.179.22.87	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.180.150.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl79 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
45.79.89.188		147.237.72.167	ishurim.aka.idf.i	NULL Character in Method [[#22]][[#3]][[#1]][[#2]][[#0]][[#1]][[#0]][[#1]]ü[[#3]][[#3]]Ub½Á*ÈÛNJð+[[#15]]/²÷[[#28]]º³<@íT£æ#(†öOp„n[[#0]][[#0]]pÀ0À,À2À.À/À+À1À-[[#0]]£[[#0]]Ÿ[[#0]]¢[[#0]]žÀ(À$À[[#20]]À	Block	1
95.240.3.94	Italy	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
40.77.167.33	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
212.199.118.124	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/an	Block	1
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
149.88.161.108	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/8/110378.pdf	Block	1
46.19.86.87	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
45.79.89.188		147.237.72.167	ishurim.aka.idf.i	Illegal Byte Code Character in Method [[#22]][[#3]][[#1]][[#2]][[#0]][[#1]][[#0]][[#1]]ü[[#3]][[#3]]Ub½Á*ÈÛNJð+[[#15]]/²÷[[#28]]º³<@íT£æ#(†öOp„n[[#0]][[#0]]pÀ0À,À2À.À/À+À1À-[[#0]]£[[#0]]Ÿ[[#0]]¢[[#0]]žÀ(À$À[[#20]]À	Block	1
212.179.22.89	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.181.110.91	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEntrance in madim.atal.idf.il/1088-he/meretz.aspx	Block	1
45.79.89.188		147.237.72.167	ishurim.aka.idf.i	Unknown HTTP Request Method [[#22]][[#3]][[#1]][[#2]][[#0]][[#1]][[#0]][[#1]]ü[[#3]][[#3]]Ub½Á*ÈÛNJð+[[#15]]/²÷[[#28]]º³<@íT£æ#(†öOp„n[[#0]][[#0]]pÀ0À,À2À.À/À+À1À-[[#0]]£[[#0]]Ÿ[[#0]]¢[[#0]]žÀ(À$À[[#20]]À in URL	Block	1

03-10-2016-12:04:07 to 03-10-2016-13:04:07