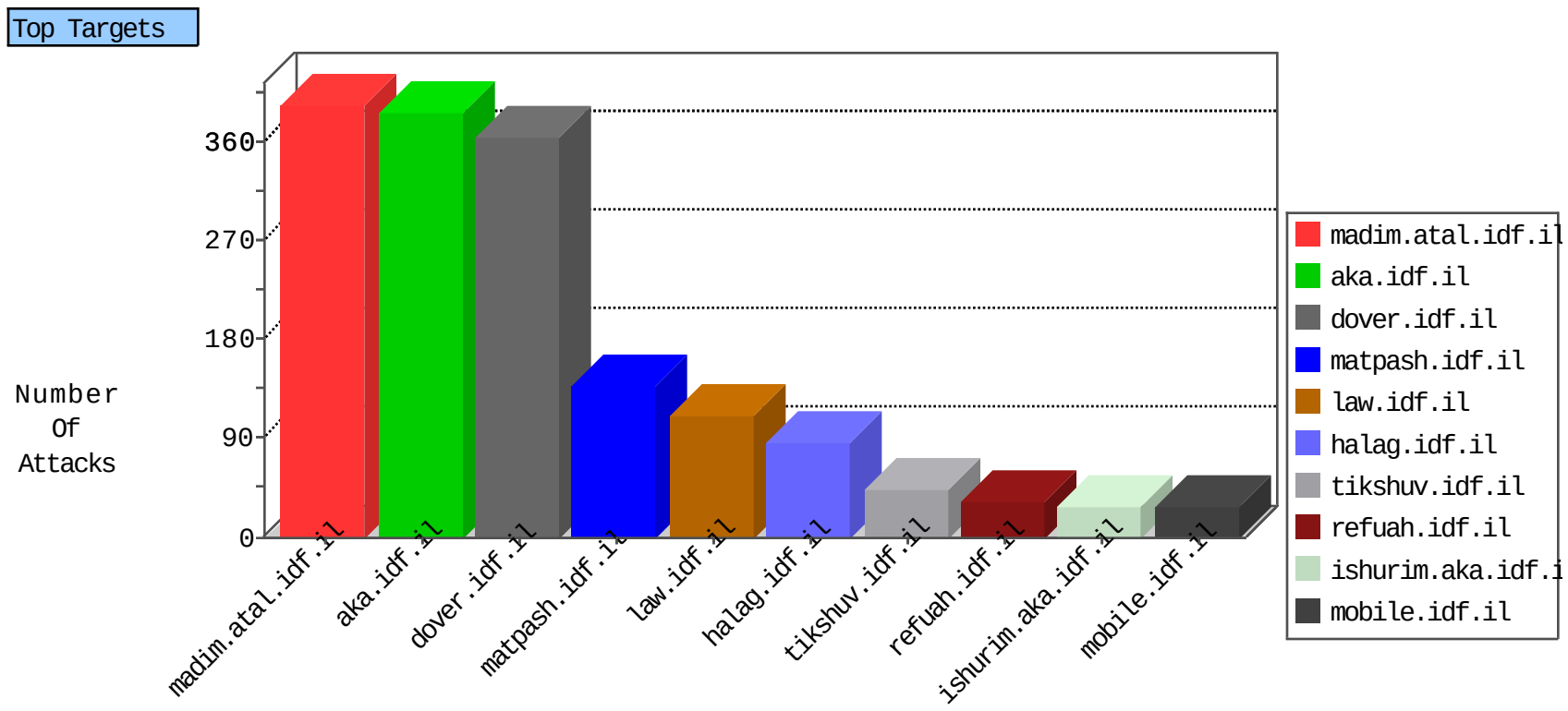
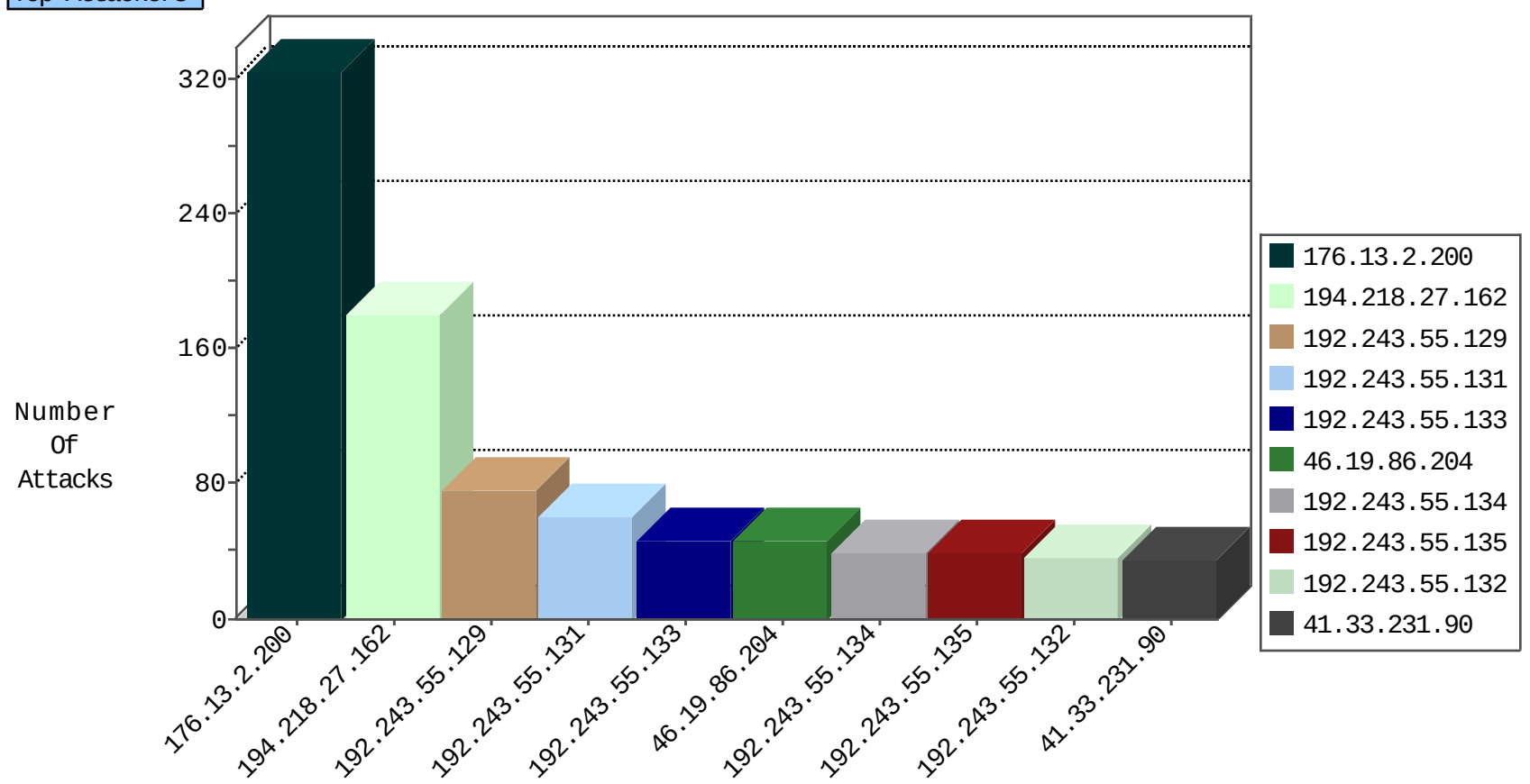
03-02-2016-21:04:01 to 03-02-2016-22:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-02-2016-21:04:01 to 03-02-2016-22:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
124.114.9.62	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
192.99.63.194	Canada	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
192.99.63.194	Canada	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
156.202.148.233		147.237.77.216	dover.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
192.99.63.194	Canada	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
27.34.90.87	Nepal	147.237.72.14	dover.idf.il(old)	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
192.99.63.194	Canada	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
188.138.102.50	Germany	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

03-02-2016-21:04:01 to 03-02-2016-22:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.126.66.233	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
213.8.10.16	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
2.54.9.81	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
80.246.130.212	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
84.109.113.16	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
61.135.189.119	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
87.71.28.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
95.86.65.164	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
5.29.75.74	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.253.220.133	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
157.55.39.210	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
207.46.13.96	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
80.246.133.249	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
107.170.68.76	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	1
52.26.202.58	United States	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

03-02-2016-21:04:01 to 03-02-2016-22:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.54.173.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.232.98.38	147.237.76.42		refuah.idf.il	ET SCAN NMAP -f -sS	1
94.102.48.193	147.237.0.19	Netherlands	madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
85.130.218.184	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
79.178.214.92	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
201.232.25.160	147.237.77.121	Colombia	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
79.178.18.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.243.55.133	147.237.77.216	Dominica	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.44.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.226.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.68.135	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.62.7	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.194.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.232.98.38	147.237.76.42		refuah.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.8.46	Canada	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
87.69.127.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.190	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
201.232.25.160	147.237.77.121	Colombia	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
79.178.50.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
201.232.25.160	147.237.77.121	Colombia	e.navy.idf.il	ET SCAN NMAP -f -sS	1
46.151.52.139	147.237.76.176	Ukraine	test.ncore.idf.i	ET SCAN NMAP -sS window 1024	1
176.13.7.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.45	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.240.64	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.232.98.38	147.237.76.42		refuah.idf.il	ET SCAN NMAP -sS window 2048	1

03-02-2016-21:04:01 to 03-02-2016-22:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.2.200	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	160
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	120
176.13.2.200	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	80
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	60
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
205.236.144.4	Canada	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
37.46.39.35	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
109.65.82.38	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
156.205.197.254		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
79.181.186.115	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
85.65.192.68	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
5.28.156.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.210.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.137	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
66.249.66.129	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.129	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	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.121	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
192.243.55.131	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence		monitor	6
37.142.206.59	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.225.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.45	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.32.79	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.129	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.183.225.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.247	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.19.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.45	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.129	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.54.50.52	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.247	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.225.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
185.32.179.1	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
46.19.86.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.200	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
5.102.215.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
109.253.196.102	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
192.243.55.131	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.2.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
46.19.86.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	47
46.121.158.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.54.41.127	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
176.13.2.200	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	3
46.118.155.216	Ukraine	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
109.160.173.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.15.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
108.170.88.202	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.24.30	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
84.111.201.191	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/	Block	3
199.30.24.57	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.86.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.178.50.178	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	3
199.30.25.66	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.86.88	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.86.88	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
142.54.85.170	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
79.181.186.115	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.64.234	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1407-he/atal.aspx	Block	1
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xgf5b3nolwrvy3ncdghpa2fcbwvzahvsyxzcdgfryw5vdf9oyxrhyxz1cmfcmi5wzgy=&infocenteritem=true	Block	1
166.172.62.81	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
104.58.22.154	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.44.139.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/faq.aspx&sa=u&ved=0ahukewie9tj846llahvjbswkhsqya6uqjbaidw&usg=afqjcnefysu6yi5sb7zbjwsjmdbowklaxw	Block	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/promotional_videos.asp	Block	1
74.12.36.232	Canada	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.118.155.216	Ukraine	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version _pk_ses.20.8afc=*	Block	1
109.253.196.102	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
2.54.46.167	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
82.81.81.210	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.81.81.210	Block	1
66.249.64.239	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1409-he/atal.aspx	Block	1
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/kesher	Block	1
173.208.136.170	United States	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
37.38.34.59	Kuwait	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.76.123.188	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ved in www.aka.idf.il/main/sachar/klali.aspx	None	1
77.125.144.251	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl75 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
180.76.15.12	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9736-he/refuah.aspx	Block	1
46.120.104.81	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_id.20.8afc=5bd3abeb53d54ea5.1451581306.13.1456946541.1456946541.;	Block	1
2.54.140.96	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
82.81.81.210	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/images/tofes106/	Block	1
66.249.66.75	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/yohalan/main/main.asp	Block	1
173.208.136.170	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
109.65.82.38	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
37.46.39.35	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
212.106.71.35	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.178.19.36	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl61 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/facts.asp	Block	1