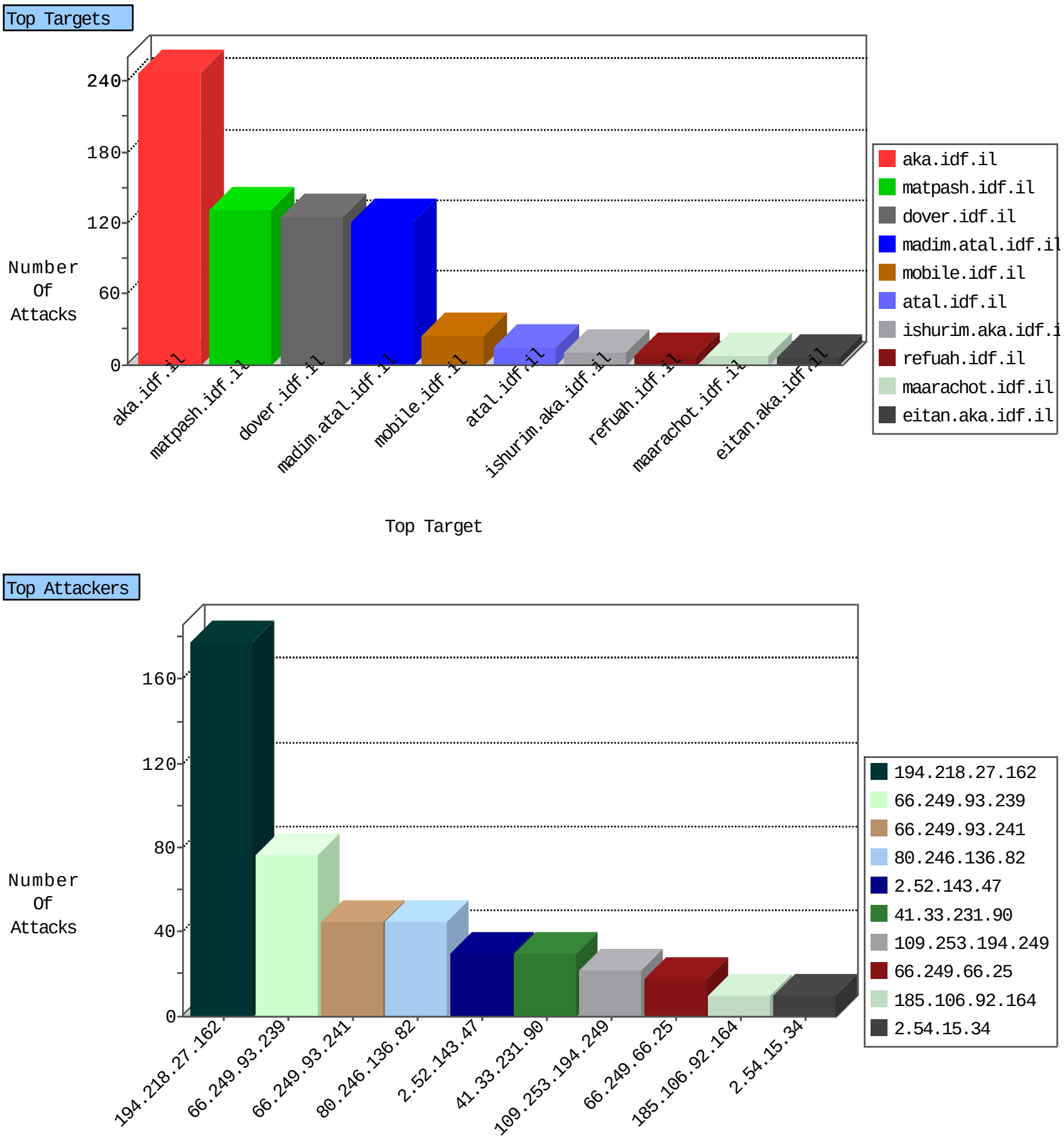
03-02-2016-07:04:02 to 03-02-2016-08:04:02

IDF Under Attack
Daily Report



03-02-2016-07:04:02 to 03-02-2016-08:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.181.46	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
81.211.8.238	Europe	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
47.88.103.153	Canada	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1
192.99.63.194	Canada	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
47.88.103.153	Canada	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	drop	1
184.105.139.80	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.2	United States	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.108	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
40.85.142.106	United States	147.237.76.197	e.himush.idf.il	JLM_Purple_Con_Limit_Http	drop	1

03-02-2016-07:04:02 to 03-02-2016-08:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.0.143	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
51.255.65.87	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
51.255.65.72	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

03-02-2016-07:04:02 to 03-02-2016-08:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
113.76.90.199	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
93.113.125.11	147.237.77.178	Romania	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
46.151.52.139	147.237.72.217	Ukraine	e.idf.il	ET SCAN NMAP -sS window 1024	1
189.254.90.133	147.237.76.38	Mexico	e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
189.254.90.133	147.237.76.38	Mexico	e.e.meitav.idf.il	ET SCAN NMAP -f -sS	1
185.72.179.221	147.237.77.226		www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.221	147.237.77.176		matpash.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.221	147.237.76.86		navy.idf.il	ET SCAN Potential SSH Scan	1
113.76.90.199	147.237.77.243	China	mobile.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
95.35.209.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.110.192.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.36	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
189.254.90.133	147.237.76.38	Mexico	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
187.75.48.23	147.237.76.39	Brazil	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.72.179.221	147.237.77.216		dover.idf.il	ET SCAN NMAP -sS window 1024	1
185.72.179.221	147.237.76.147		chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.221	147.237.76.44		e.refuah.idf.il	ET SCAN Potential SSH Scan	1

03-02-2016-07:04:02 to 03-02-2016-08:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	118
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	59
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
66.249.93.239	United States	147.237.77.176	matpash.idf.il	drop		drop	24
66.249.93.239	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
66.249.93.239	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
66.249.93.241	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
66.249.93.241	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
66.249.93.239	United States	147.237.77.176	matpash.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	10
217.132.123.166	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
66.249.93.241	United States	147.237.77.176	matpash.idf.il	drop		drop	8
66.249.93.241	United States	147.237.77.176	matpash.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	7
2.52.25.110	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.21.24	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.23.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.221.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.242.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
94.230.86.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.50.127.138	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
94.230.86.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.135.103	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.93.241	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.219	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.177.128.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.163	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.136.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.141.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.235.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.84.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.160.242.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
93.113.125.11	Romania	147.237.77.170	maarachot.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.147.240	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
87.69.211.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.44.95	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
2.54.22.11	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
66.249.93.239	United States	147.237.77.176	matpash.idf.il	Directory Traversal	directory traversal overflow	monitor	2
2.54.44.95	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
79.177.217.184	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
5.22.135.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.54.44.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
80.246.130.239	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
195.160.242.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
66.249.93.241	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
213.244.118.251	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
85.250.21.207	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
2.54.44.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
2.52.143.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
109.253.194.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
66.249.66.25	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	18
2.54.15.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
2.54.148.24	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	4
109.253.223.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.148.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.69.221.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.190.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.22.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.130.9	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.54.148.24	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.148.24	Block	2
46.19.85.252	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
185.80.220.24		147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/cgi-bin/php	Block	1
95.86.70.10	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/421-2258-he/patzar.aspx&sa=u&ved=0ahukewj0i_-1qkhlahwoo5okhf3taxkqfggrmam&usg=afqjcngd7sy4jf1c6zw04e95dxuialvoaa	Block	1
79.177.3.184	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl55 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
217.194.204.8	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
54.213.197.191	United States	147.237.72.167	ishurim.aka.idf.i	NULL Character in URL	Block	1
66.249.93.239	United States	147.237.77.176	matpash.idf.il	Distributed URL is Above Root Directory	Block	1
54.200.74.228	United States	147.237.76.31	nakchal.idf.il	Illegal Byte Code Character in Method	Block	1
185.99.32.3		147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.67.199.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.15.34	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/mobile/templates/basket/basket.aspx	Block	1
79.177.217.184	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
217.194.207.188	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
54.213.197.191	United States	147.237.72.167	ishurim.aka.idf.i	Unknown HTTP Request Method µñWß)[[#20]]0éJ[[#14]]¨ in URL	Block	1
113.76.90.199	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
93.113.125.11	Romania	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
54.200.74.228	United States	147.237.76.31	nakchal.idf.il	NULL Character in Method	Block	1
207.46.13.107	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.54.15.34	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
79.180.17.202	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
65.55.210.25	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
113.76.90.199	China	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
94.199.151.22	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 94.199.151.22	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
54.213.197.191	United States	147.237.72.167	ishurim.aka.idf.i	Illegal Byte Code Character in Method µñWß)[[#20]]0éJ[[#14]]¨	Block	1
217.194.195.86	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.220.222	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1498-he/atahttp:/192.118.60.6/radio/2015/03/31/6287826.mp3l.aspx	Block	1
46.19.85.236	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
176.13.21.24	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
94.199.151.22	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
77.237.138.202	Czech Republic	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /	Block	1
217.194.199.199	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
54.213.197.191	United States	147.237.72.167	ishurim.aka.idf.i	Illegal Byte Code Character in URL	Block	1
109.253.221.249	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.39	United States	147.237.77.74	law.idf.il	Parameter Type Violation SearchText in www.law.idf.il/163-6639-he/patzar.aspx	Block	1