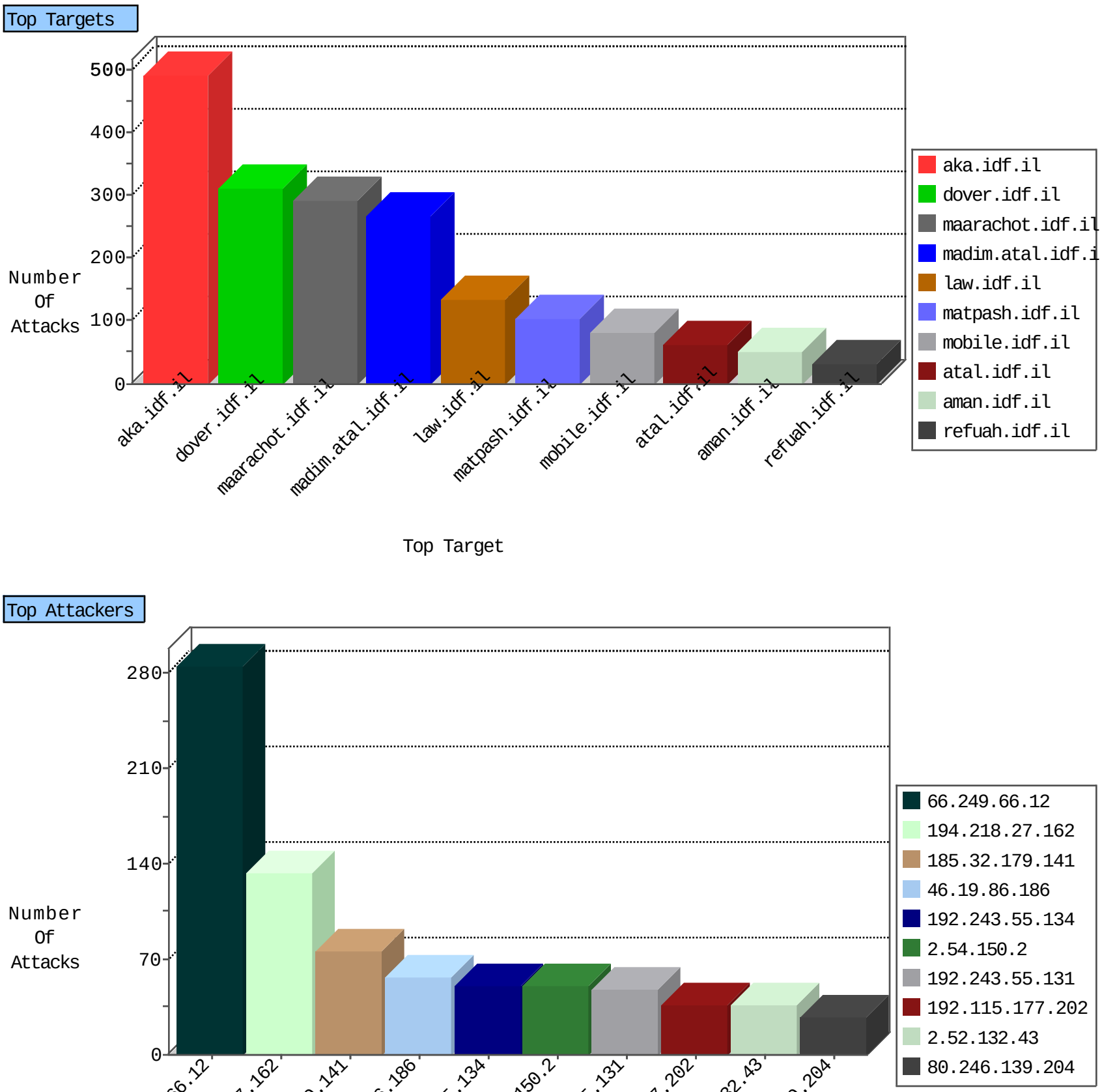
03-02-2016-15:04:03 to 03-02-2016-16:04:03

IDF Under Attack
Daily Report



03-02-2016-15:04:03 to 03-02-2016-16:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.151.36.231	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	6
82.145.218.12	Europe	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	5
37.142.64.47	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
192.168.0.22		147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
46.19.85.36	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
192.99.63.194	Canada	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
46.184.68.203	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
164.132.54.194	Italy	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
81.218.56.125	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
185.25.205.117	Italy	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
217.64.195.236	Italy	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1

03-02-2016-15:04:03 to 03-02-2016-16:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.139.158.209	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.66.134.252	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
51.255.65.53	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
51.255.65.78	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
173.208.136.170	United States	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Block	1
51.255.65.47	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
51.255.65.52	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

03-02-2016-15:04:03 to 03-02-2016-16:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	286
77.127.165.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.44.133.108	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 2048	1
62.219.99.154	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.229.115	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.132.58.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.31	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.172.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.149.149	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.250.183.40	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
2.54.171.173	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.109.198	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.152.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
188.120.154.147	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.24	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
120.72.118.152	147.237.76.30	Vietnam	himush.idf.il	ET SCAN NMAP -sS window 2048	1
79.182.144.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
120.72.118.152	147.237.76.30	Vietnam	himush.idf.il	ET SCAN NMAP -f -sS	1
79.177.194.146	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.121.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.44.133.108	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -f -sS	1
46.117.62.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.138.215.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.135.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.49	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
86.242.239.208	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
208.80.155.214	147.237.77.74	United States	law.idf.il	Tehila - Perl LWP with fake user agent	1
37.26.149.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.116.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.72.14	Sweden	dover.idf.il(old	ET SCAN NMAP -sS window 1024	1
2.54.169.223	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.106.152	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.0.19	China	madim.atal.idf.i	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
80.246.136.135	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
120.72.118.152	147.237.76.30	Vietnam	himush.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.154.244	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
114.215.111.222	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1

03-02-2016-15:04:03 to 03-02-2016-16:04:03

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	88
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	46
192.115.177.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
37.26.149.147	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.253.213.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
80.246.139.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
66.249.81.183	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
66.249.81.157	United States	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	10
176.13.15.183	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.134	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.81.179	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	9
176.13.15.183	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
85.130.254.75	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.139.47	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.134	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
85.130.254.75	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
85.130.254.75	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.225	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
66.102.9.115	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	7
80.230.228.240	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.225	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.169.146	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.126.253.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.62.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.210.188.49	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.103	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.128.48.84	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.29.193.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.134.159	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	6
192.243.55.134	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
80.246.139.204	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.131	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.129	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.139.204	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.131	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.130.69	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
192.243.55.134	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.137	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5

03-02-2016-15:04:03 to 03-02-2016-16:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
46.19.86.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
2.54.150.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
2.52.132.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
79.181.54.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
66.249.66.25	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	9
85.64.109.198	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.64.109.198	Block	9
2.54.184.145	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	7
38.111.147.88	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 38.111.147.88	Block	4
66.249.81.218	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
185.32.179.54	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 185.32.179.54	Block	3
109.253.213.150	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.35.138.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.182.155.51	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
80.246.136.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
157.55.2.148	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	2
2.54.139.47	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
185.32.179.54	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
111.94.83.250	Indonesia	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.21.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.153.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.199.218.50	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.54.14.199	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
81.218.55.253	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
78.40.177.35	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.39.40	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
192.162.26.4	Spain	147.237.72.166	aka.idf.il	NULL Character in Method ^v[[#3]]ÑÇµq[[#17]]Â¸ì0÷ÎC–O˜0[[#20]]æ2Ö=øÎÔ'é[[#28]]L•Rtj[[#3]]Îªy™[[#4]][[#25]]×íê[[#5]]Gúš58É[[#19]];:]$´DÏÐ·>?¼[[#11]]/‰Þÿðÿ ZVÃLŠÅ 7Q–œHŸMæñ´6µË[[#26]]õv/&GÏ´ü[[#19]]Ïéq`=Ñ[[#24]][[#8]]Ý“‘S#012å'0å•õ}ÂÕEaÀ[[#23]]8•lBdšÚäŽh¸ï2[[#19]][[#5]][[#4]]v¶çr¬÷•éëj`°šÐ§¼?#012Q3½â>nitº[[#17]]7vQóù¤p1¾Z€<[[#28]]ñ)¶~¨Ý8³ö[[#31]]à![[#8]]¿•©[[#31]]ÎìÈ[[#0]]èÿ™à•«Øä•}EµÄ[[#8]][[#20]]Œ*yq1[[#2]]Ž[[#2]]u•N•R[[#2]]H4Œ%™Ofÿ›!6s8æùŠî[[#14]]4[[#8]]*J€ŸGüxÏL¤¼9±O"V	Block	1
54.200.74.228	United States	147.237.77.235	sviva.idf.il	Malformed URL	Block	1
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 192.162.26.4	Block	1
87.71.91.245	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.152.247.1	Germany	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx	Block	1
66.249.81.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
196.3.37.251	Brazil	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
54.213.177.200	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method	Block	1
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 192.162.26.4	Block	1
81.218.55.253	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
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Illegal URL Path Encoding [[#31]].p•q›a[[#11]][[#2]]a¬Êu%ybm¸ixt¸ m[[#20]]k3p…ozwt[[¸ U/¥#28£™]]71#[[r]]'9]]7#[[’›·uÊŒ"}¡÷	Block	1
23.81.248.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
185.118.27.12		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.180.160.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.15.183	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
66.249.66.75	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_	Block	1
192.162.26.4	Spain	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
54.200.74.228	United States	147.237.77.235	sviva.idf.il	NULL Character in Header Name at	Block	1
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 192.162.26.4	Block	1
89.138.73.27	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1

03-02-2016-15:04:03 to 03-02-2016-16:04:03