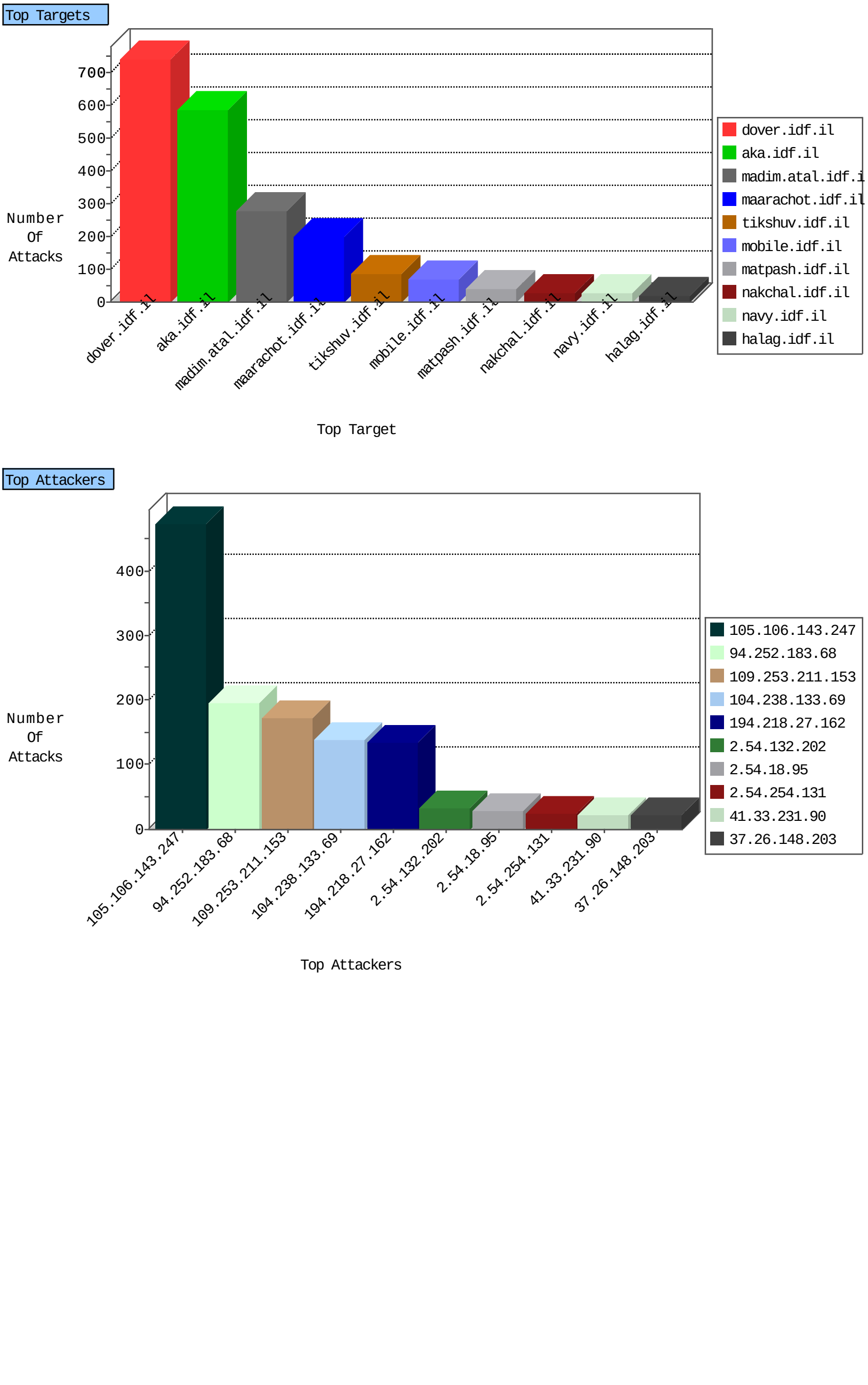
02-29-2016-12:04:05 to 02-29-2016-13:04:05

IDF Under Attack
Daily Report



02-29-2016-12:04:05 to 02-29-2016-13:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	2500
104.238.133.69		147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	137
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	99
82.145.211.191	Europe	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	20
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
212.199.241.250	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
24.234.216.180	United States	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1
24.234.216.180	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1
184.105.247.195	United States	147.237.77.234	halag.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

02-29-2016-12:04:05 to 02-29-2016-13:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
193.43.245.250	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
213.8.204.30	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
193.43.246.250	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
188.120.151.217	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
2.54.168.72	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
217.132.149.227	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
31.154.159.218	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
207.46.13.85	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
212.235.40.29	Israel	147.237.72.166	aka.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
66.249.64.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

02-29-2016-12:04:05 to 02-29-2016-13:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.67.190.134	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	3
105.106.143.247	147.237.77.216	Algeria	dover.idf.il	SQL Injection - Select From	3
105.106.143.247	147.237.77.216	Algeria	dover.idf.il	ET SCAN NMAP -sS window 1024	2
46.121.92.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
46.19.85.210	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.120.126.122	147.237.72.166		aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.223.171	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
148.251.21.227	147.237.72.166	Germany	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.2.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
128.30.52.71	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
105.106.143.247	147.237.77.216	Algeria	dover.idf.il	portscan: TCP Distributed Portscan	1
82.102.146.154	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.29.203.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.47.247	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
189.202.241.84	147.237.76.176	Mexico	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
46.19.85.200	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.120.126.95	147.237.72.166		aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.68.86	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
139.196.198.206	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.139.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.196.146	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.86.123.204	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.194.203.125	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

02-29-2016-12:04:05 to 02-29-2016-13:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
94.252.183.68	Syrian Arab Republic	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	107
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	90
94.252.183.68	Syrian Arab Republic	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	88
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	45
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
37.26.148.203	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	21
2.54.254.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
37.218.214.215	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
217.132.18.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.60.49	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
46.19.86.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.145.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.94.102.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.22.129.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.168	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.90.45.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.27.105.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.165.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.81.31.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.188.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.130.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.86.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.19.176.18	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
62.0.41.2	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.178.218.176	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
139.196.198.206	China	147.237.76.38	e.e.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.168	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.26.146.186	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.30	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.54.254.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.146.186	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.26.146.186	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.26.146.186	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.93.252	Israel	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
37.26.146.186	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
2.54.55.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.23.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.26.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.156.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.15.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.8.118.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.0	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.252	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
109.65.138.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-29-2016-12:04:05 to 02-29-2016-13:04:05

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
37.26.148.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.114.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-29-2016-12:04:05 to 02-29-2016-13:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.211.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	173
2.54.132.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
46.19.86.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
37.26.146.195	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	14
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.106.143.247	Block	14
2.54.155.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
2.54.18.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
5.29.230.226	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	7
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	6
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	6
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	6
192.115.90.26	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1746	Block	6
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	6
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	6
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	5
82.166.239.100	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	5
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	5
148.251.21.227	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	4
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	3
176.13.17.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.117.136.6	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
197.33.31.117	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.213.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1379-he/dover.aspx parameter PageNum	Block	2
2.54.15.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.115.90.26	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 192.115.90.26	Block	2
109.66.33.98	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in www.aka.idf.il/main/giyus/questionnaire.aspx	None	2
79.183.114.235	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
213.151.43.108	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21461-he/dover.aspx&sa=u&ved=0ahukewj2ppqa4pzlahxikcwkhrazbxuqfggsmam&usg=afqjcne6ultmubarn2bcl_7b7nlu_yeirw	Block	2
5.29.157.217	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1806-he/dover.aspx	Block	2
109.253.140.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1824-he/dover.aspx	Block	2
37.26.148.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
148.251.21.227	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 148.251.21.227	Block	2
46.19.86.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
178.216.202.190	Poland	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php	Block	1
37.26.146.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1780-he/dover.aspx	Block	1
82.80.33.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	1
75.39.96.163	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	NULL Character in Method	Block	1
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1133-he/dover.aspx	Block	1
213.57.54.215	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/7/109107.pdf	Block	1
66.249.64.229	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1239-he/atal.aspx	Block	1
95.153.129.178	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation &l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
185.3.144.56	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucNewsFlashControl$txtSearch in www.idf.il/1153-he/dover.aspx	Block	1
40.77.167.27	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1842-he/dover.aspx	Block	1

02-29-2016-12:04:05 to 02-29-2016-13:04:05