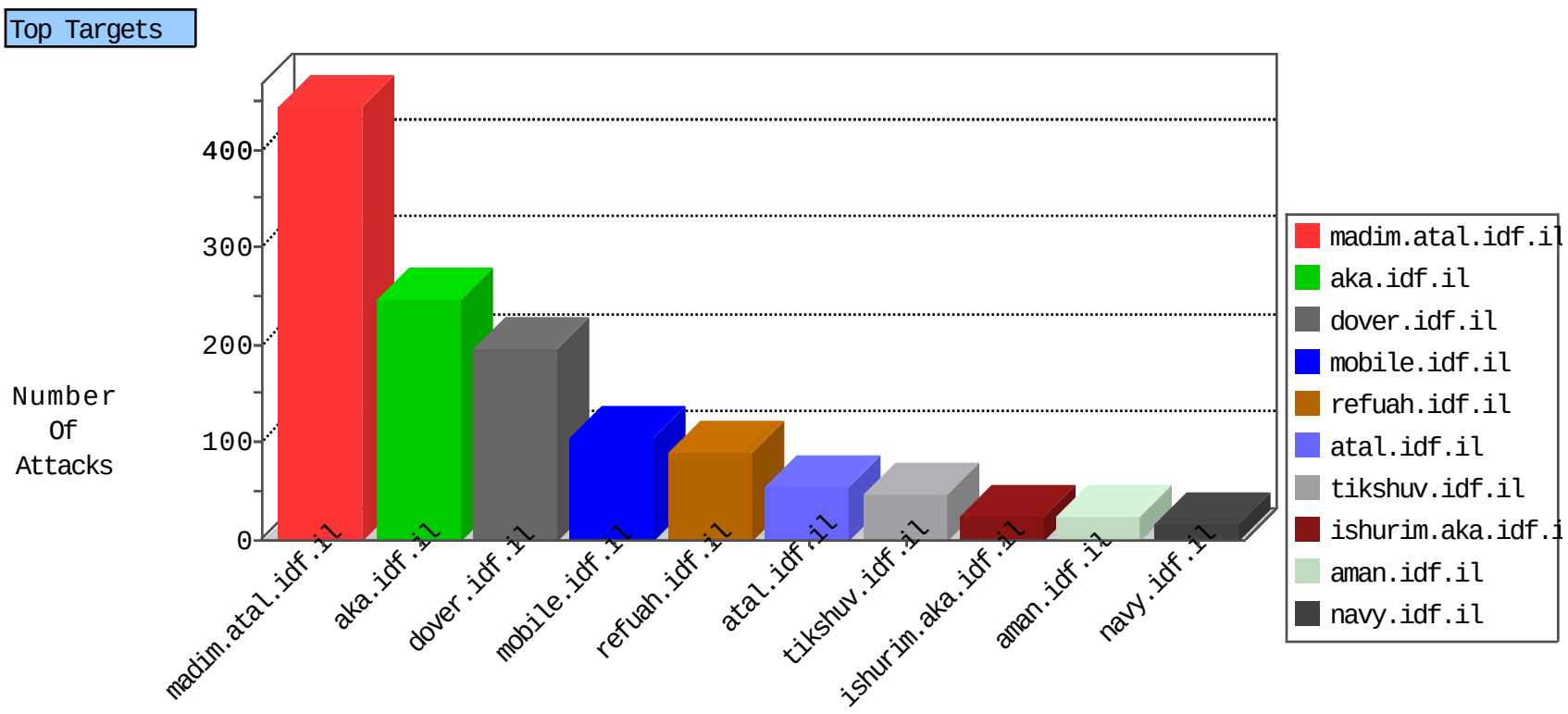
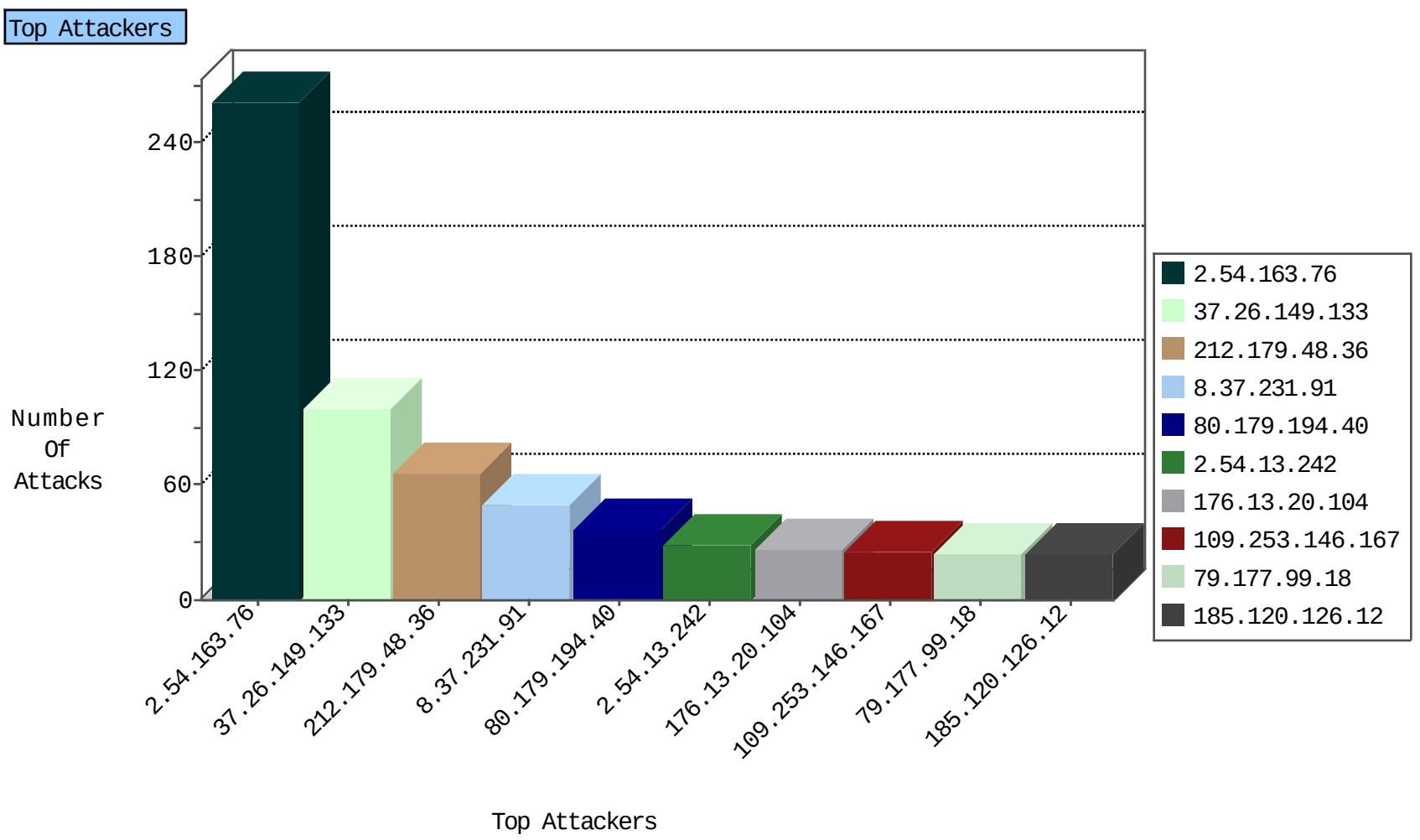
03-10-2016-15:04:06 to 03-10-2016-16:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-10-2016-15:04:06 to 03-10-2016-16:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
8.37.231.91	Anonymous Proxy	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
8.37.231.91	Anonymous Proxy	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
89.248.172.207	Netherlands	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
14.120.237.148	China	147.237.72.217	e.idf.il	Block_Udp_All_Nets	drop	1
198.20.70.114	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.21	United States	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.207	Netherlands	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1
42.127.172.162	Japan	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1
81.218.56.125	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.207	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
12.162.142.14	United States	147.237.77.226	www.chamatz.aka.idf.il	L4 Source or Dest Port Zero	drop	1
89.248.172.207	Netherlands	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
71.6.135.131	United States	147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	1

03-10-2016-15:04:06 to 03-10-2016-16:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.202.39	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	20
79.177.118.182	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
5.29.127.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
176.13.0.75	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
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	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.79.234	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
188.166.239.76	Russian Federation	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
66.249.79.241	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
112.74.67.70	China	147.237.77.205	prisha.idf.il	0543: HTTP: php.cgi Access	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-10-2016-15:04:06 to 03-10-2016-16:04:06

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	2
66.249.79.43	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
46.19.85.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.44.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.24.215	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
74.102.103.58	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
62.17.136.66	147.237.72.166	Europe	aka.idf.il	portscan: TCP Distributed Portscan	1
185.3.147.225	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
121.141.225.10	147.237.77.216	Korea, Republic of	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.166.93.182	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.7.188	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

03-10-2016-15:04:06 to 03-10-2016-16:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.48.36	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	66
80.179.194.40	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
185.120.126.12		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
176.13.20.104	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
8.37.231.91	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
8.37.231.91	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
79.182.186.130	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.85.26	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
80.246.133.119	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
37.26.147.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.90.193.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
79.177.99.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.177.99.18	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
188.120.154.47	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
77.125.109.41	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
2.54.62.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
122.151.188.177	Australia	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.54.48.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
213.151.44.156	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
95.86.119.126	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
176.13.5.49	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.227	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.6.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.12.197	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
125.21.244.34	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
80.179.194.40	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.169.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.188.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.154	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.253.129.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.198.175	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.130.232.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.130.232.5	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
125.21.244.34	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.147.216	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.147.216	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
125.21.244.34	India	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
125.21.244.34	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
37.26.149.133	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		monitor	4
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.130.222.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.199.218.50	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.176.172.176	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
77.125.92.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.232.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.27.106.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-10-2016-15:04:06 to 03-10-2016-16:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.163.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	262
37.26.149.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
2.54.13.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
109.253.146.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
2.52.35.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.22.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
157.55.2.160	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
199.30.16.182	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
81.218.152.66	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.218.152.66	Block	4
46.254.21.136	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.254.21.136	Block	3
2.54.33.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.150.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.20.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.135.92	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
109.253.199.107	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.253.199.107	Block	2
80.178.227.165	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.180.123.146	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
109.253.199.107	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
80.179.194.40	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	2
81.218.152.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Illegal Byte Code Character in Method žuòÒaŠ#012-ëä¥=Np5ÂKLFC³~!B	Block	1
37.26.147.214	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CaptchaText in mobile.idf.il/authentication/login	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	NULL Character in URL ><«s [[#31]]m#[[#28]][[#8]][[#28]]•[[#0]][[#0]]f[[#30]]r€¾”b!jך3†× [[#20]]¨[[#8]],	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
137.226.113.7	Germany	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
68.180.228.112	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
199.203.186.77	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/2974.jpg	Block	1
94.230.93.73	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.239.68.30	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/css/icons/icons.woff	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
80.246.130.87	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
79.180.150.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl27 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.199.154.194	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Illegal HTTP Version	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
185.25.151.159	Poland	147.237.77.235	sviva.idf.il	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	1
82.80.28.123	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.254.21.136	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Malformed URL	Block	1
37.26.147.214	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Unknown HTTP Request Method T[[#17]]ÒÐ«î-/"¤¡©®î¥>`Ã[[#23]]Å‹B in URL ><«s [[#31]]m#[[#28]][[#8]][[#28]]•[[#0]][[#0]]f[[#30]]r€¾”b!jך3†× [[#20]]¨[[#8]],	Block	1
79.180.150.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl87 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
212.179.22.81	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
138.134.102.16	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/headerupper/	Block	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/3365.jpg	Block	1
184.105.247.196	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1

03-10-2016-15:04:06 to 03-10-2016-16:04:06