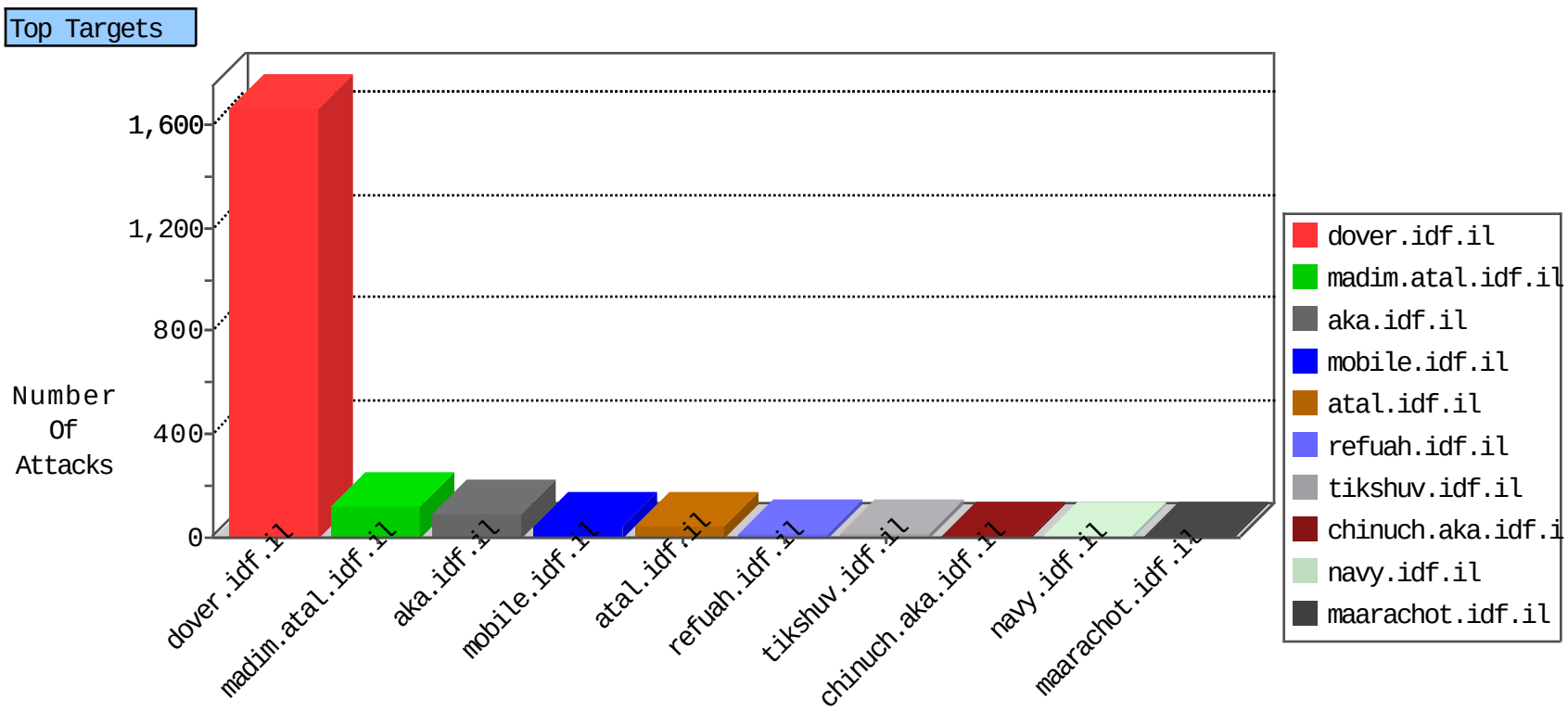
03-12-2016-10:04:06 to 03-12-2016-11:04:06

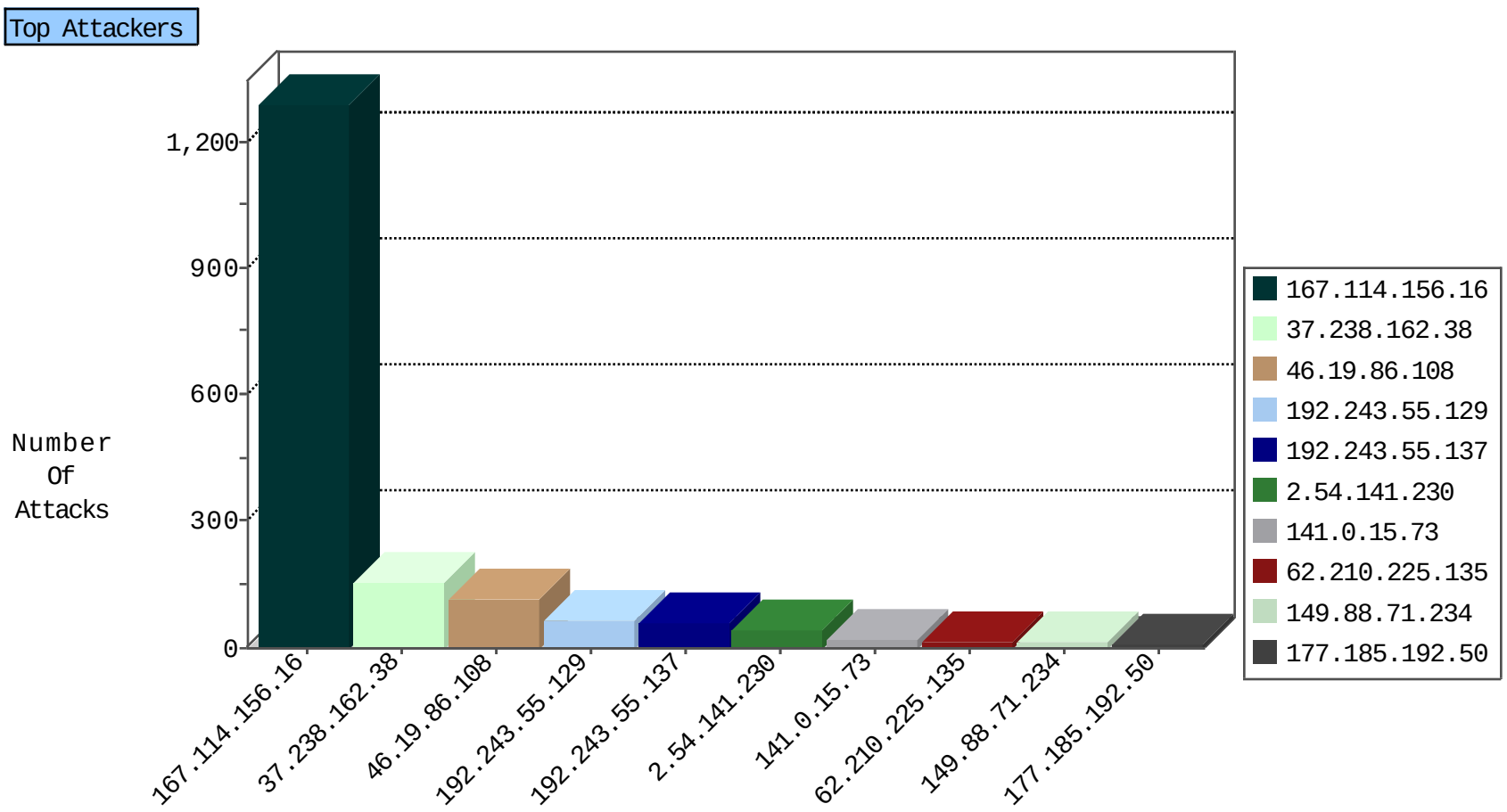
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

03-12-2016-10:04:06 to 03-12-2016-11:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4000
46.19.86.108	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	263
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
66.249.64.190	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
184.105.247.195	United States	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
162.248.100.195	United States	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
184.105.139.70	United States	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.41	United States	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1
216.218.206.81	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
162.248.100.195	United States	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.78	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.206	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
216.218.206.113	United States	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
162.248.100.195	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.118	United States	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1
126.46.7.121	Japan	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1

03-12-2016-10:04:06 to 03-12-2016-11:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.225.135	France	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
177.185.192.50	Brazil	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
108.59.8.80	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-12-2016-10:04:06 to 03-12-2016-11:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.210.225.135	147.237.77.233	France	atal.idf.il	SQL Injection - Select From	12
177.185.192.50	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.65.224	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
193.105.134.220	147.237.76.147	Sweden	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
164.39.11.198	147.237.8.46	United Kingdom	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.172.140	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
61.216.84.147	147.237.76.44	Taiwan	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
195.142.106.5	147.237.0.34	Turkey	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
93.189.26.18	147.237.76.148	Austria	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.172.140	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
218.57.11.7	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
195.142.106.5	147.237.0.35	Turkey	akaws.idf.il	ET SCAN Potential SSH Scan	1
195.142.106.5	147.237.0.15	Turkey	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

03-12-2016-10:04:06 to 03-12-2016-11:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.238.162.38	Iraq	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	78
37.238.162.38	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	78
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
141.0.15.73	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
2.54.141.230	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.54.141.230	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	8
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.116.190.250	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
109.253.203.209	Israel	147.237.0.34	tikshuv.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.178.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.147.140	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.141.230	Israel	147.237.77.243	mobile.idf.il	SYN Attack		reject	4
109.67.225.71	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.54.141.230	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.54.141.230	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.210.247.171	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
2.54.177.180	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.141.230	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
79.178.61.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.107.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.57.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.3.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.167.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.22.130.103	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.127.240.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.0.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.22.135.116	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.182.141.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.90.143.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.164.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.234.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.210	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
5.29.248.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
185.3.147.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

03-12-2016-10:04:06 to 03-12-2016-11:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
2.54.141.230	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	2
87.71.118.241	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 87.71.118.241	Block	2
79.182.187.60	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
41.44.238.110	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.241	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.asmx/getjs	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	NULL Character in URL /[[#7]]8jÛ™`[[#30]]ע	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding /[[#7]]8jÛ™`[[#30]]ע	Block	1
37.239.70.3	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
93.172.242.151	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
184.105.247.196	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pa in www.aka.idf.il/giyus/forum/asp/showforum.asp	None	1
46.19.85.66	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version __atuvs=56e3d9182a2a7074000; _pk_id.20.8afc=a267b61b8a048e3e.1457772844.1.1457772844.1457772844.; _pk_ses.20.8afc=*	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 149.88.71.234	Block	1
149.78.57.12	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
87.71.80.169	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	1
156.207.239.23		147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.128.50.218	United States	147.237.77.74	law.idf.il	Admin Blocking	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Malformed URL	Block	1
41.44.93.62	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.67.132.92	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl89 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
192.116.190.250	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.66.29	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1273-he/atal.aspx	Block	1
46.19.85.66	Israel	147.237.77.216	dover.idf.il	Malformed URL __atuvc=1	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 149.88.71.234	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
176.13.3.224	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.13.3.224	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/8/3338.jpg	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 149.88.71.234	Block	1
41.44.116.212	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.67.132.92	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$tfasimSignAll in www.aka.idf.il/main/sachar/payslips.aspx	None	1
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
46.19.85.66	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method nId=331jjlbglugq2kqv3tkguj45; in URL __atuvc=1	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 149.88.71.234	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /[[#7]]8jÛ™`[[#30]]ע	Block	1
2.54.150.160	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
87.71.118.241	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/0/	Block	1
176.13.3.224	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/sahar/default.aspx	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
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 149.88.71.234	Block	1
130.185.155.74	Sweden	147.237.77.74	law.idf.il	PHP Attempt	Block	1
84.58.7.21	Germany	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.69.133.242	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter fb709480 in aka.idf.il/giyus/	None	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 149.88.71.234	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version •[[#8]]†j•ýÒ·[[#1]]D-B»Æ3[[#1]]óc“ô; !ö[[#22]]Î˜õ4ßZUö{»&[[#18]]¹8è)¦J\’ëbbÃ[[#28]]÷[[#20]]{J{·)®ÀOhHT4»ß[[#22]]D ›üQ‰•œú>@¯e<BÕp,[[#23]][[#11]][[#18]]†¼Î%²W†A!>÷[[#14]][[#25]]Pñ®Žˆÿ}.öc„[[#11]]‰gÀ[[#12]]0Âùr@Þ¨[[#18]]h6rË[[#5]][[#22]]ÆŒ[[#4]]ë9[[#8]]Ô[[#1]]-[[#22]]•N[[#11]]uvË[[#4]]§nß[[#4]]—],_]1kLËV}¹[[#2]]•LÍå*¡,N"Ãš~][[#24]]	Block	1
5.22.135.116	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 5.22.135.116	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/dover.aspx.	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-9122-he/kkkkkkk=8f177212kkkkkkk_8f177212	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/3/69383.pdf	Block	1
46.19.85.66	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1

03-12-2016-10:04:06 to 03-12-2016-11:04:06