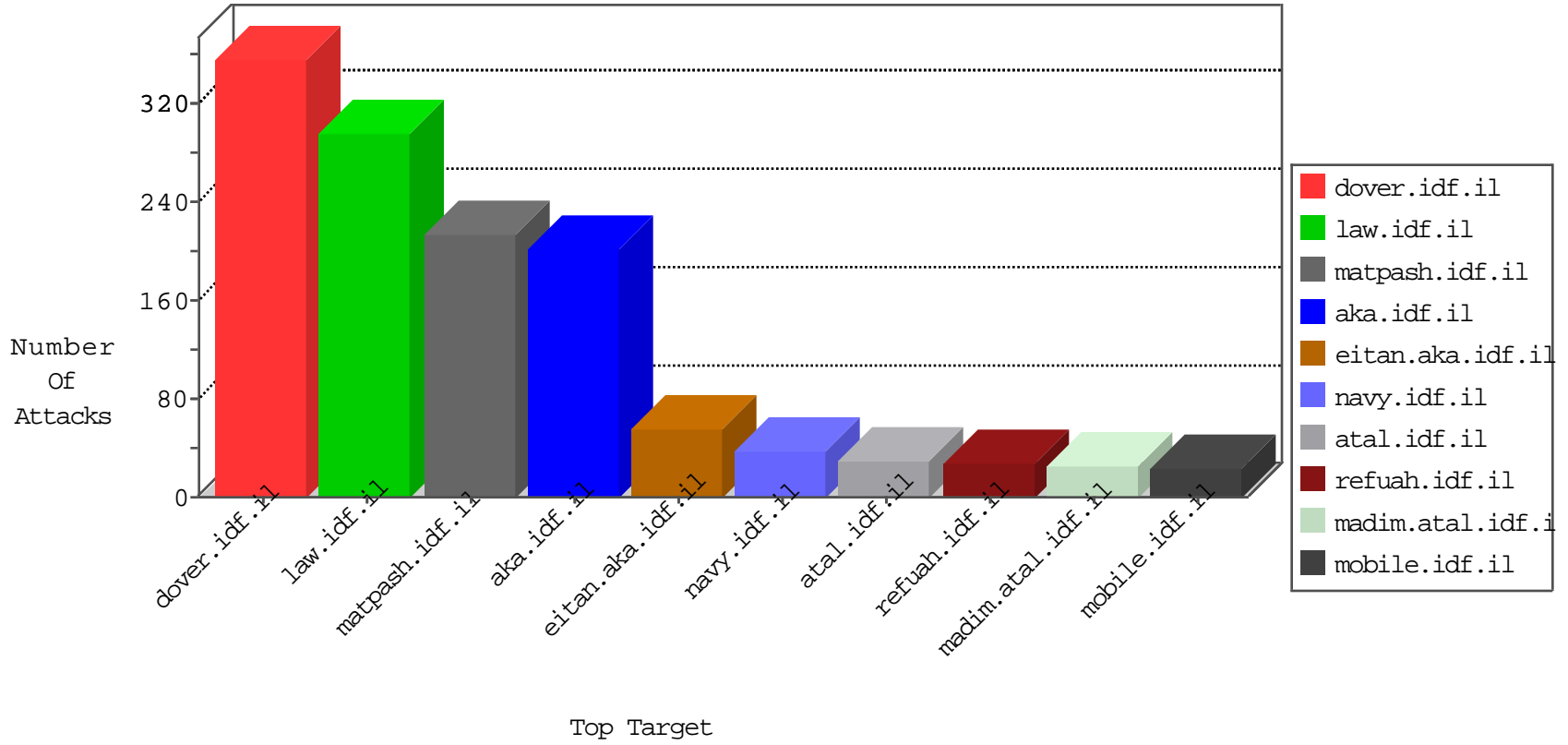


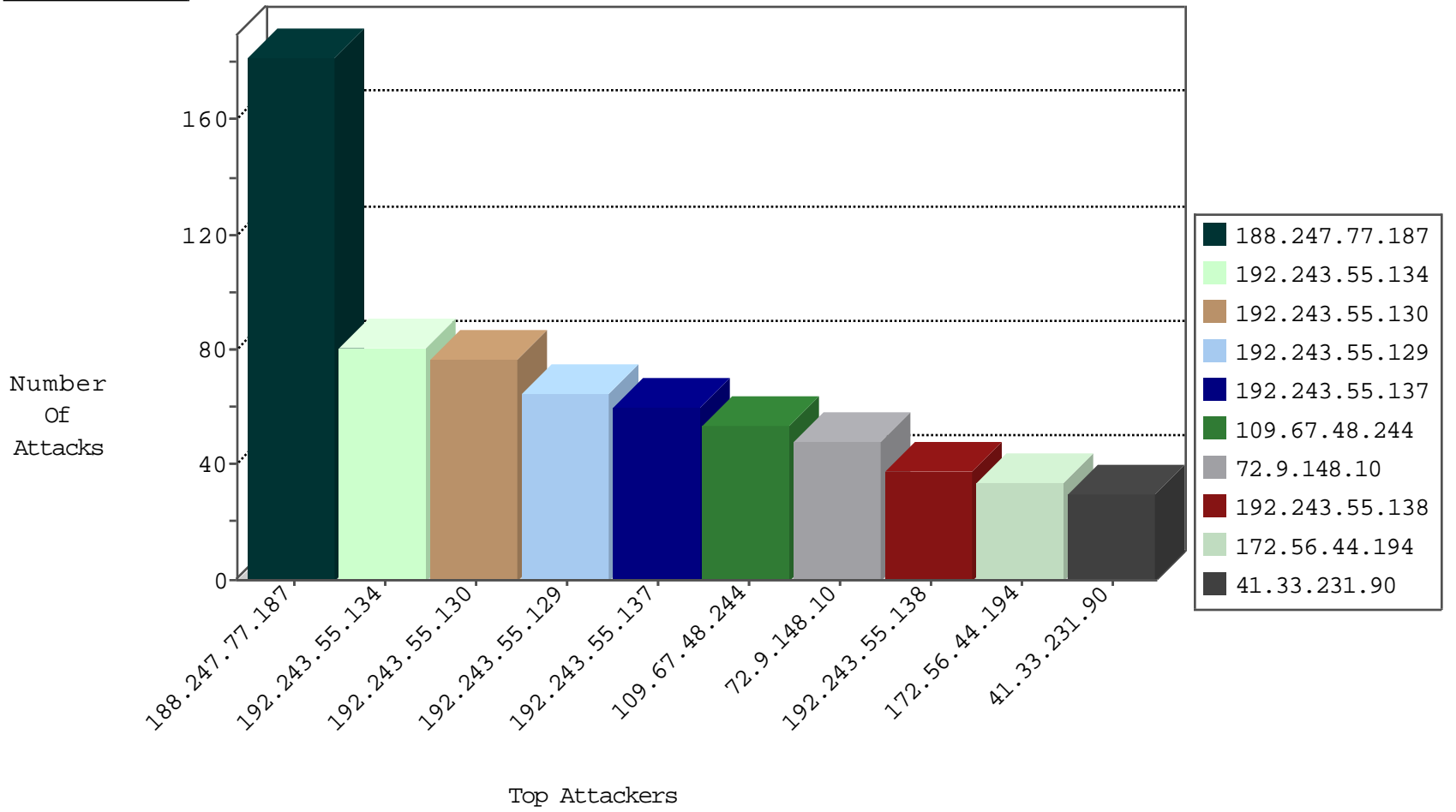
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.54.237	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
183.60.48.25	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
123.151.42.61	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
185.130.5.201		147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.201		147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.201		147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.245.33.104	Netherlands	147.237.77.176	matpash.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
194.88.154.138	Poland	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
213.57.128.210	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
5.102.254.233	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
109.66.3.142	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
84.245.33.104	Netherlands	147.237.77.176	matpash.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
194.88.154.138	Poland	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
103.21.58.191	India	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
89.19.29.90	Turkey	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
89.19.29.90	Turkey	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
84.245.33.104	Netherlands	147.237.77.176	matpash.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
89.19.29.90	Turkey	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
89.98.3.81	Netherlands	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	2
69.167.186.64	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	2
66.249.66.47	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
106.39.60.189	China	147.237.8.46	e.chinuch.idf.i	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
------------------	----------------	------------------	------	-----------	-------

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
188.247.77.187	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	182
109.67.48.244	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	48
172.56.44.194	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	24
109.253.205.212	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
79.183.227.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
195.74.38.14	Sweden	147.237.77.233	atal.idf.il	drop	SAM rule	drop	14
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
98.19.222.133	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	12
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
37.26.149.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
2.54.185.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.96.128.60	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	12
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.132	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
79.176.162.87	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	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	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.134	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.129	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.121.89.194	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.50	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.23.107	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.29.253.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.9.126	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.135.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.64.107.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
120.52.72.47	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.176.65.150	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
2.54.144.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.175.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.65.87.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.65.53.185	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Questio n\$78 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	3
84.110.109.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.29.43.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.151.45.64	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/113201.pdf&sa=u&ved=0ahukewith5o5nyfl ahxh83ikhfobb_wqfggpam&usg=afqjcnhoetj7djlwgtflultbi9h5hwo6za	Block	2
95.86.98.14	Israel	147.237.76.39	mobile.meitav.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPassword in mobile.meitav.idf.il/templates/login.aspx	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	1
85.65.20.191	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
199.115.117.88	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/admin/basic	Block	1
40.77.167.57	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
109.226.49.124	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.65.53.185	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Questio n\$3 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
79.183.154.104	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
213.151.45.64	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 213.151.45.64	Block	1
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/core/doc_mgr/mce_src=	Block	1
109.67.175.58	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
199.115.117.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/admin/basic	Block	1
50.62.161.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
109.253.205.212	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout2.css	Block	1
109.65.53.185	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Questio n\$35 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
84.108.27.33	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Questio n\$34 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19239-en/dover.aspx http://digg.com/submit	Block	1
17.138.56.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.56.26	Block	1
109.67.226.81	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
85.130.192.48	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Questio n\$81 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
200.59.205.238	Argentina	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	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/1/2971.jpg	Block	1
128.232.110.28	United Kingdom	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
84.108.95.93	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.243.55.137	Block	1
37.26.149.185	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.67.226.81	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
200.59.205.238	Argentina	147.237.72.166	aka.idf.il	Multiple signatures from 200.59.205.238	Block	1
162.144.123.57	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
109.65.53.185	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Questio n\$98 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
198.58.102.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
40.77.167.44	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
109.160.234.109	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
109.65.53.185	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Questio n\$14 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
207.46.13.193	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx	None	1