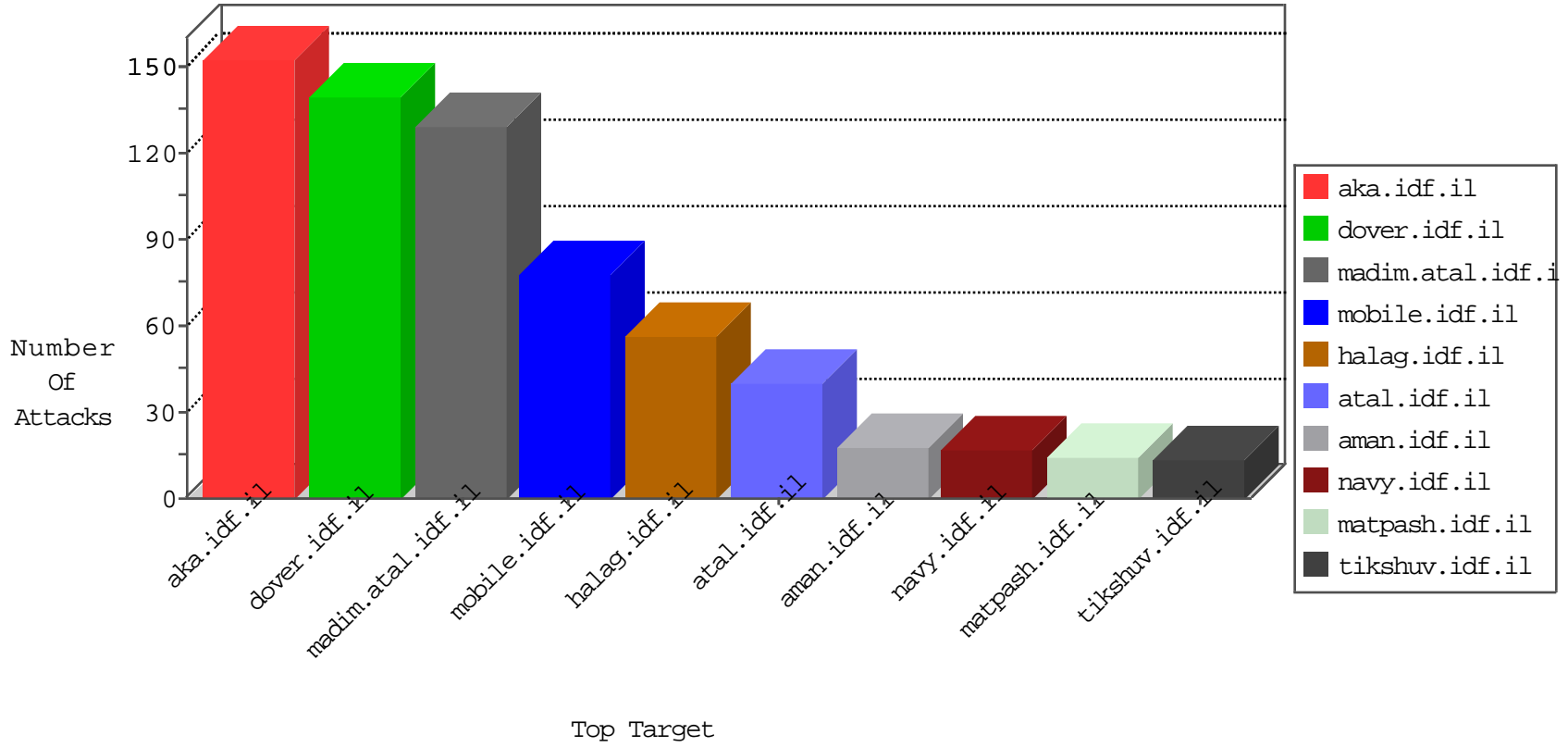


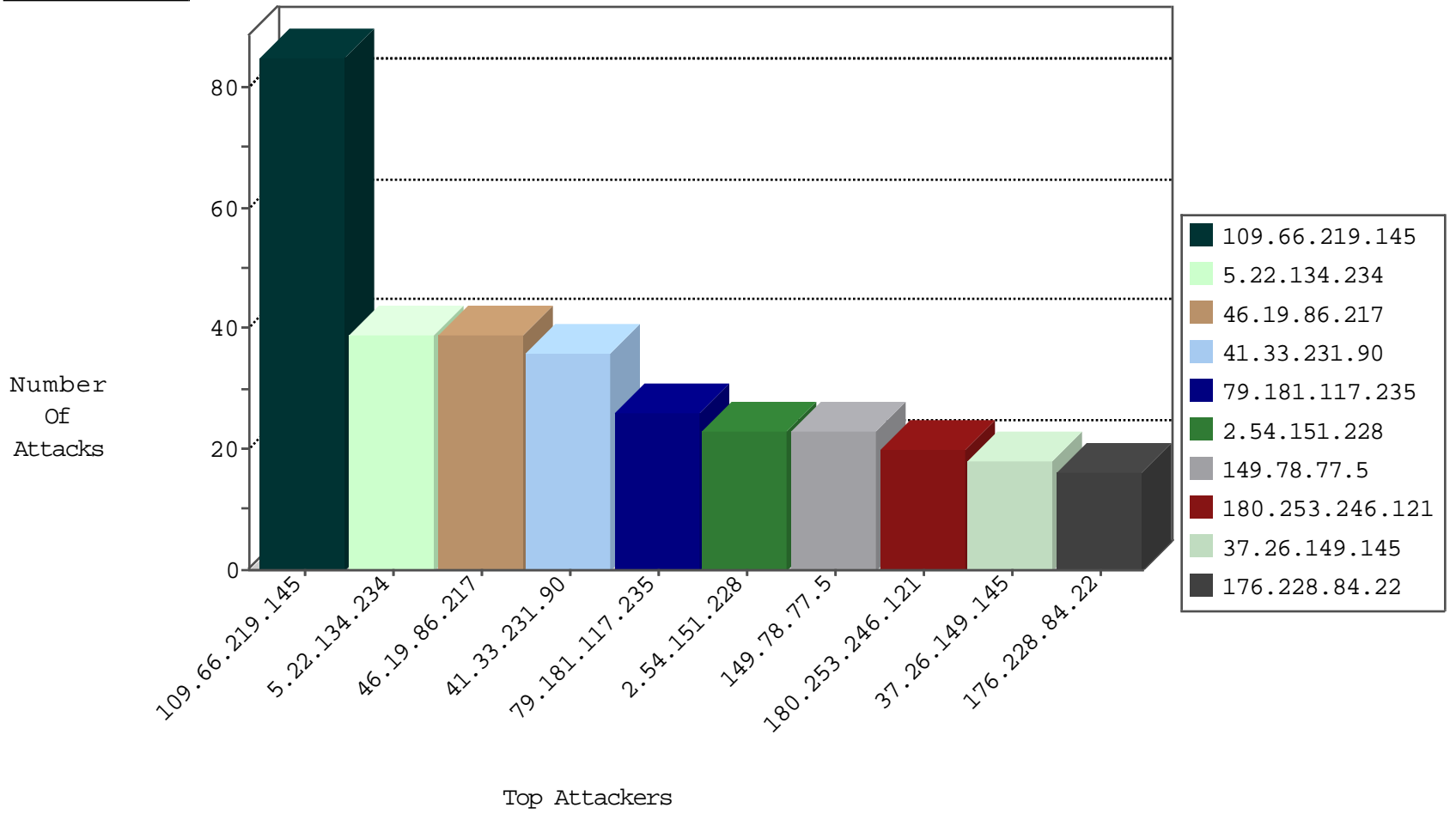
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
217.26.171.188	Moldova, Republic of	147.237.77.176	matpash.idf.il	I4 Source or Dest Port Zero	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
134.147.203.115	Germany	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	2
71.6.158.166	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
205.209.185.11	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
220.134.149.19	Taiwan	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1
205.209.185.11	United States	147.237.72.156	aman.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
183.2.172.45	China	147.237.77.61	e.cogat.idf.il	I4 Source or Dest Port Zero	drop	1
205.209.185.11	United States	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
65.196.137.3	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	1
205.209.185.11	United States	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.122.1	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
37.26.147.161	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
149.78.99.234	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
84.94.41.65	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
51.255.65.22	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
51.255.65.59	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

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	4
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
191.248.83.29	147.237.76.30	Brazil	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.99.148.50	147.237.77.216	Korea, Republic of	dover.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.76.201	Ukraine	e.atal.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
191.248.83.29	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
149.78.8.48	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
91.201.236.113	147.237.76.201	Ukraine	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
213.14.168.240	147.237.76.30	Turkey	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.22.134.234	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
79.181.117.235	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
180.253.246.121	Indonesia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
2.54.151.228	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.178.163.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.183.129.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.228.84.22	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
176.228.84.22	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	7
84.228.213.52	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.77.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
5.28.188.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.13.152	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
109.226.44.156	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.18.109	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
122.162.167.115	India	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.214.85	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.102.9.65	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.0	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
109.64.63.230	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	5
37.26.149.145	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
37.26.149.145	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.26.149.145	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.214.85	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.234	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.179.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.246.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.167.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.234.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.77.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.181.194.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.196.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.77.5	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.0	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.128.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
149.78.77.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.182.126.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.144.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.94.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.81.44.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.66.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.51.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.77.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.219.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
46.19.86.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	9
2.54.151.228	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
219.94.128.197	Japan	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 219.94.128.197	Block	5
2.54.134.198	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	4
46.19.86.111	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
149.78.8.48	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 149.78.8.48 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	2
2.54.18.109	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
194.30.134.180	Cyprus	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/kamlar/klali/default.asp	None	1
113.76.90.154	China	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to 147.237.76.147/	Block	1
63.246.134.230	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to /admin	Block	1
213.57.192.176	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.57.192.176	Block	1
176.13.13.152	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.181.117.235	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
217.69.133.230	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
194.30.134.180	Cyprus	147.237.72.166	aka.idf.il	Unknown Parameter docid in ww.aka.idf.il/sites/klali/default.asp	None	1
74.82.47.2	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
213.57.192.176	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
176.228.84.22	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
84.228.97.143	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
194.30.134.180	Cyprus	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
149.78.60.161	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
77.125.128.218	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.125.128.218	Block	1
213.57.192.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
5.22.134.234	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
194.30.134.180	Cyprus	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/brothers/contact/	None	1
89.138.96.214	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
46.19.86.234	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
194.98.203.210	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.39	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
77.125.128.218	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	1
216.218.206.66	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
37.26.147.216	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
194.30.134.180	Cyprus	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/brothers/skira/default.asp	None	1
46.120.182.205	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
157.55.39.188	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
79.179.211.232	Israel	147.237.72.166	aka.idf.il	Unknown Parameter y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
217.69.133.228	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/home/default.aspx	Block	1