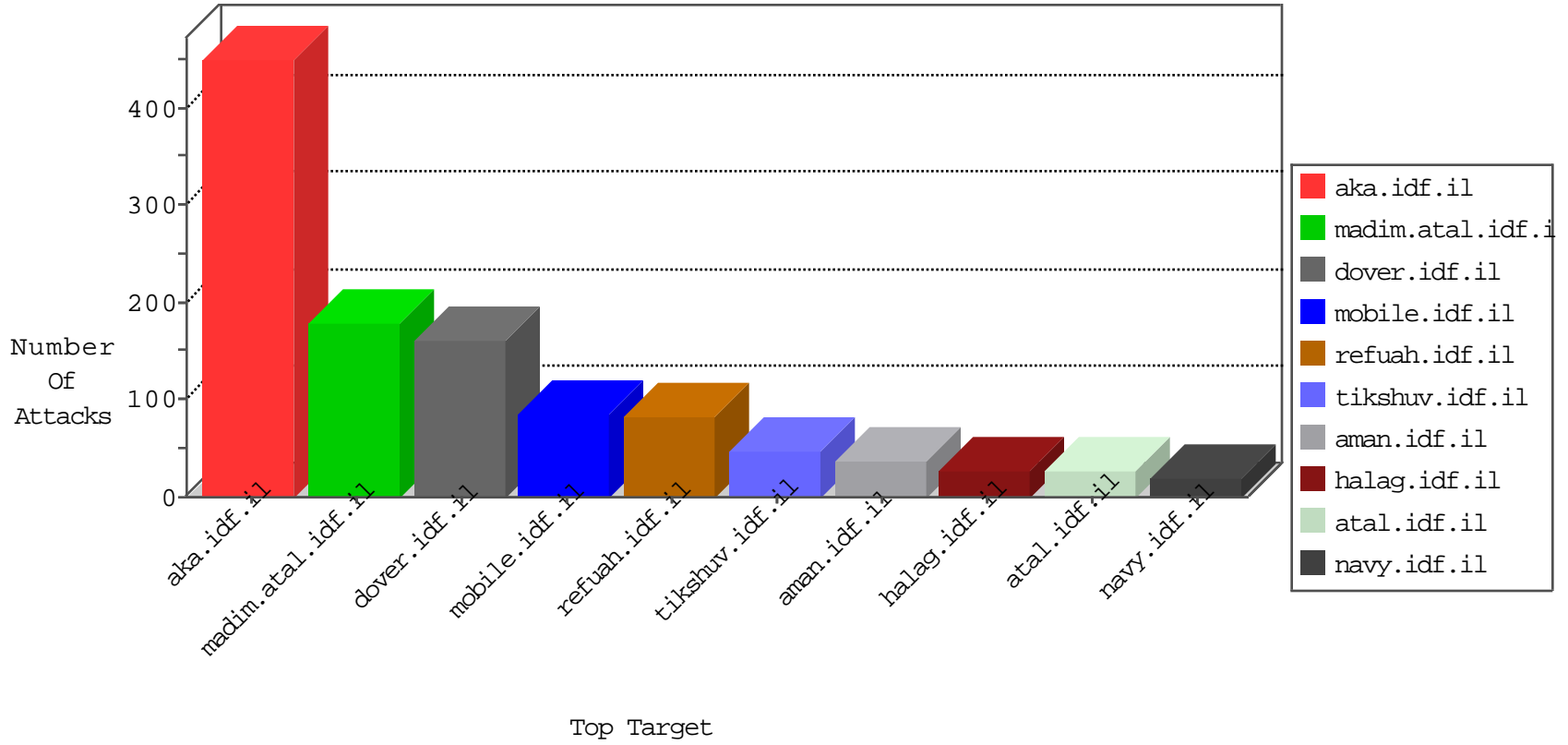


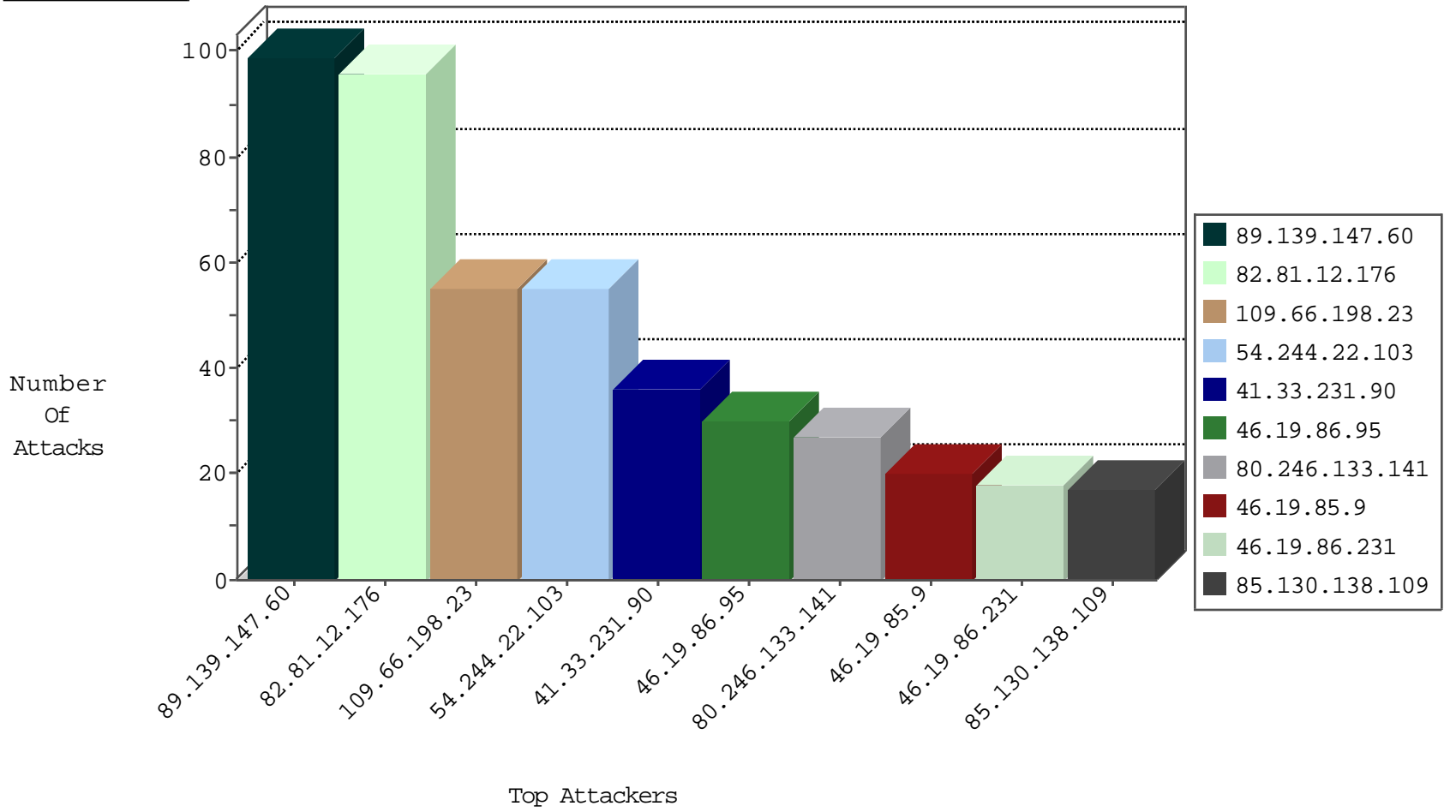
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	96
79.179.164.197	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
79.178.147.144	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
79.176.119.165	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
79.178.147.144	Israel	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
149.202.73.219	Germany	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
219.146.149.246	China	147.237.0.19	madim.atal.idf.il	Frk_Under_Attack_Con_Tcp	drop	1
124.232.150.230	China	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

01-30-2016-20:04:04 to 01-30-2016-21:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.68.125	China	147.237.77.216	dover.idf.il	C103: 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	3
66.249.81.144	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.121	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
146.0.75.114	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
79.179.128.212	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
60.173.149.204	147.237.76.39	China	mobile.meitav.idf.il	SERVER-WEBAPP JBoss JMXInvokerServlet access attempt	1
187.245.105.123	147.237.8.14	Mexico	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
182.16.64.15	147.237.77.235	Hong Kong	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
168.62.238.153	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
146.0.75.114	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.191.209	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
60.173.149.204	147.237.76.30	China	himush.idf.il	SERVER-WEBAPP JBoss JMXInvokerServlet access attempt	1
182.16.64.15	147.237.77.235	Hong Kong	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
182.16.64.15	147.237.77.235	Hong Kong	sviva.idf.il	ET SCAN NMAP -f -sS	1
168.62.238.153	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.66.198.23	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	33
80.246.133.141	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	22
46.19.85.9	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
46.19.86.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
212.76.121.166	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
2.54.136.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
94.199.151.22	United Kingdom	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.130.138.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
172.58.96.156	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
77.126.24.178	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
5.28.188.120	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
197.132.255.18	Egypt	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.46.38.142	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
213.57.209.113	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.176.59.224	Israel	147.237.0.34	tikshuv.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
109.253.200.171	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.113	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.136.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.121.252.19	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.34	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
31.210.188.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.210.186.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
188.120.148.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.160.199.102	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
109.64.161.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.210.188.8	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.73	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
188.161.49.151	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
109.186.180.99	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
31.154.148.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.107	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.121.90.8	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.148	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.210.174.66	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	4
2.52.181.163	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	4
46.19.85.73	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.52.52.177	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
185.120.126.77		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.171.67	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.179.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.151	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.80.149.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.139.147.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
46.19.86.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
2.52.185.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
85.65.116.27	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	12
109.253.141.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
46.19.86.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
85.65.100.83	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
84.108.0.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.179.179.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.29.228.130	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.29.228.130	Block	3
2.52.153.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.139.147.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
89.139.147.60	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.0.255	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
46.19.86.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
149.88.56.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.228.117.99	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
79.178.138.77	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatgauntity.aspx	Block	2
109.66.200.150	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
46.116.214.66	Israel	147.237.72.166	aka.idf.il	Unknown Parameter IsPDFForm in www.aka.idf.il/main/sachar/viewpayslip.aspx	None	1
171.25.193.77	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
109.67.127.207	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
95.86.105.41	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.86.105.41	Block	1
46.121.123.29	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.121.123.29	Block	1
182.101.129.170	China	147.237.76.147	chinuch.aka.idf.il	Unauthorized Method OPTIONS for www.chinuch.aka.idf.il/	None	1
79.182.56.143	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
46.116.214.66	Israel	147.237.72.166	aka.idf.il	Unknown Parameter IsPDF in www.aka.idf.il/main/sachar/viewpayslip.aspx	None	1
149.50.124.107	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.252.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.125.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.126.24.178	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
64.251.27.99	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to /robots.txt	Block	1
5.29.43.182	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	1
46.116.214.66	Israel	147.237.72.166	aka.idf.il	Unknown Parameter IsPDFForm in www.aka.idf.il/main/sachar/viewpayslip.aspx	None	1
84.108.31.171	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
79.180.144.92	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
109.160.238.248	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
67.19.79.218	United States	147.237.76.30	himush.idf.il	Distributed Unauthorized URL Access on /robots.txt	Block	1
5.29.228.130	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
95.86.105.41	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20373-he/idfgdover.aspx&sa=u&ved=0ahukewjhu5brld1ka hwmshwkhdX2bu0qfggtmam&usg=afqjcnhusfhghcqbbeebgdhcfhygkfvva0a	Block	1
2.54.13.147	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
60.173.149.204	China	147.237.76.30	himush.idf.il	CVE-2013-4810: JBoss Remote Command Execution 2	Block	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
80.246.133.141	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
46.116.214.66	Israel	147.237.72.166	aka.idf.il	Unknown Parameter IsPDF in www.aka.idf.il/main/sachar/viewpayslip.aspx	None	1
46.19.85.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.66.7.138	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.107.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.48	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/3/109413.pdf	Block	1