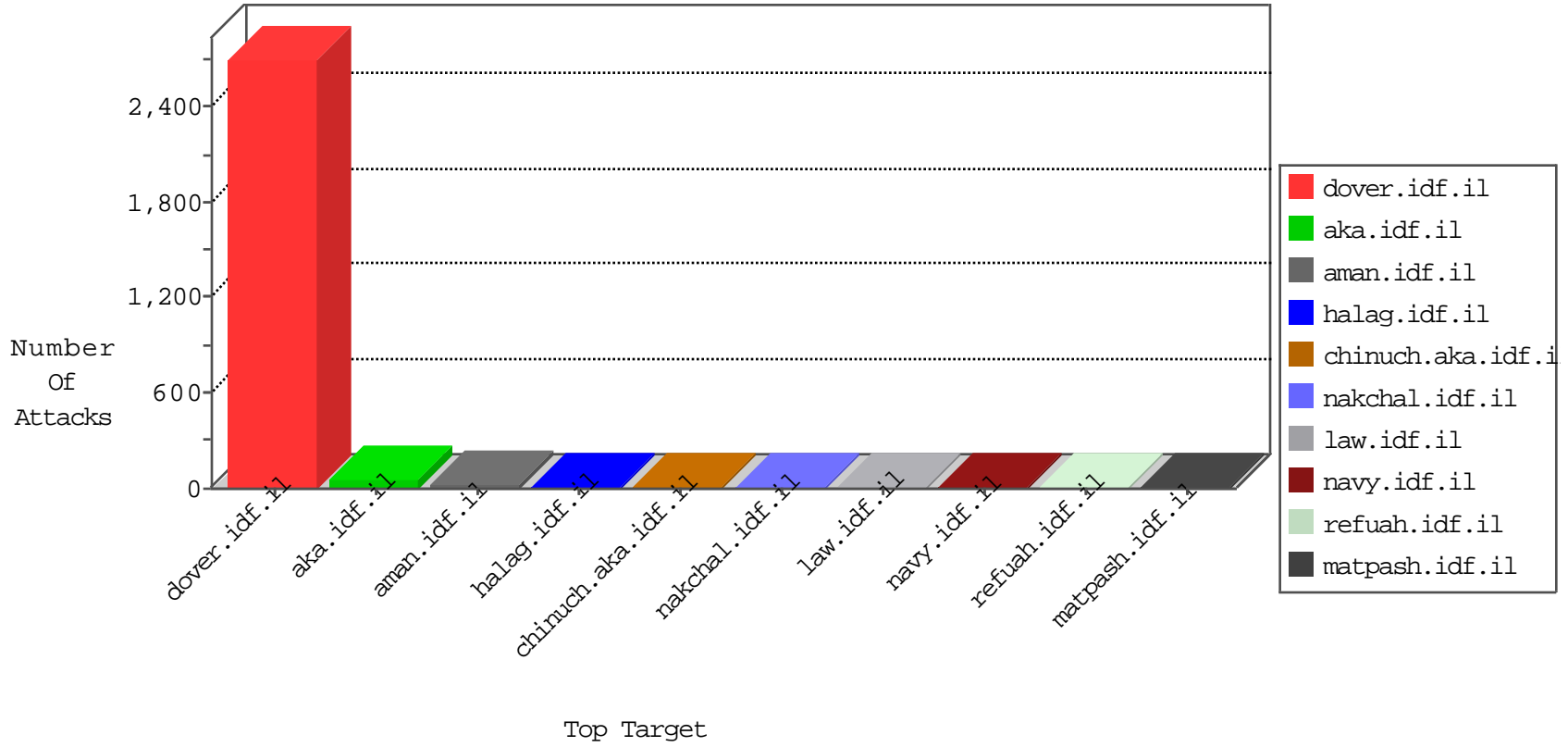


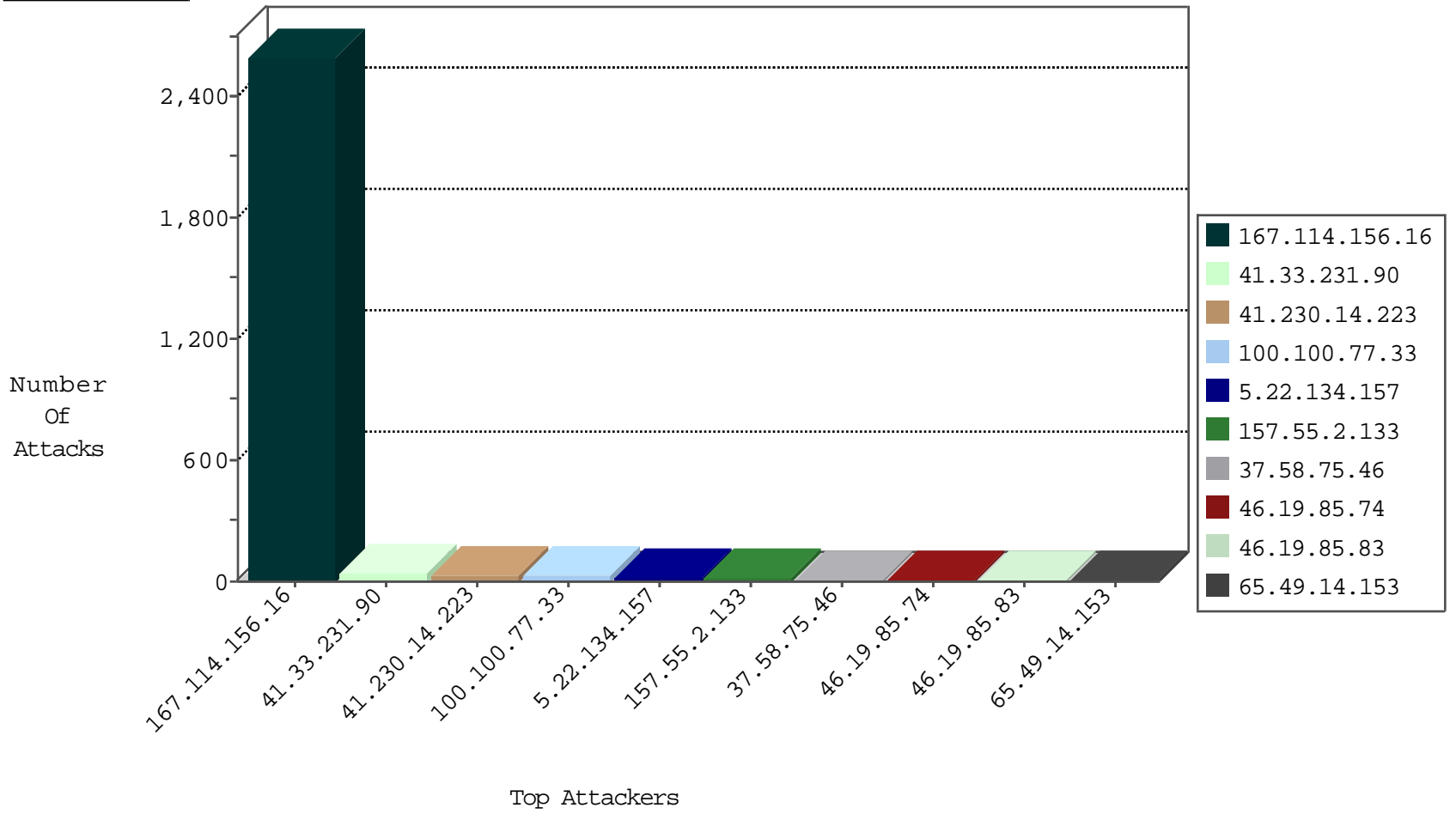
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3276
96.44.187.158	United States	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
153.254.136.181	Japan	147.237.76.38	e.e.meitav.idf.il	Invalid TCP Flags	drop	2
204.42.253.130	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	2
192.3.170.124	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
141.212.122.67	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.68	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
192.3.170.124	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
93.174.93.151	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.76.42	refuah.idf.il	block-sp-traf1	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.58.75.46	Netherlands	147.237.76.31	nakchal.idf.il	20086: HTTP: Mueblackcat Security Scanner	Block	5
37.58.75.46	Netherlands	147.237.76.147	chinuch.aka.idf.il	20086: HTTP: Mueblackcat Security Scanner	Block	4
37.58.75.46	Netherlands	147.237.76.31	nakchal.idf.il	20085: HTTP: Mueblackcat Security Scanner Initial Request	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
51.254.46.129	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN NMAP -sS window 1024	1
203.197.205.118	147.237.76.34	India	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
180.117.224.89	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
114.112.90.54	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.192.90.145	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
51.254.46.129	147.237.76.31	United Kingdom	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
37.58.75.46	147.237.76.31	Netherlands	nakchal.idf.il	ET WEB_SERVER Muieblackcat scanner	1
203.197.205.118	147.237.76.34	India	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
203.197.205.118	147.237.76.34	India	yohalan.idf.il	ET SCAN NMAP -f -sS	1
189.203.240.181	147.237.76.86	Mexico	navy.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.195	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
51.254.46.129	147.237.76.44	United Kingdom	e.refuah.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
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
100.100.77.33		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
5.22.134.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
157.55.2.133	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
65.49.14.153	Anonymous Proxy	147.237.72.166	aka.idf.il	drop		drop	6
46.19.85.74	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.183.170.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.120.139.71	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.85.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
157.55.39.247	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
188.138.17.205	France	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
141.212.121.222	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.159.237.38	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
216.218.206.94	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.96	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
149.202.47.181	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
106.38.241.106	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
74.82.47.6	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
202.112.51.96	China	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.10.99.209	Switzerland	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
5.255.253.168	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.132	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
86.161.198.197	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.110	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
64.125.239.37	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.96	United States	147.237.76.176	test.ncoore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
123.125.71.115	China	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.8	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
202.112.51.96	China	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.10.104.243	Switzerland	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
23.97.172.212	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.133	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
91.207.60.66	Ukraine	147.237.0.35	akaws.idf.il	drop		drop	1
216.218.206.122	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
64.125.239.134	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.235	United States	147.237.77.61	e.cogat.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
137.116.71.170	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.15	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
207.46.13.4	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.105	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.76	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
23.97.172.212	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	14
41.230.14.223	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	4
179.43.138.75	Switzerland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	4
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
66.249.64.177	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
84.111.124.171	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.26.148.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.43	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19474-he/idfgdover.aspx	Block	1
141.212.122.128	United States	147.237.76.147	chinuch.aka.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
31.210.189.252	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
85.159.237.38	Netherlands	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.67.138	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
195.154.146.225	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
40.77.167.36	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/Ã-â€™Ã-â„¸ çÃ-Ã ¸Ã-â„¸ çÃ-â€¸Ã-Ã ¸-â€¸Ã-Ã ¸	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation pageNum in www.idf.il/1133-he/dover.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
157.55.39.76	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/general/	Block	1
41.230.14.223	Tunisia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templ@es/navmenu/navmenu.css.aspx	Block	1
31.210.189.252	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
95.108.158.144	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.67.147	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list2005c.htm	Block	1
66.249.66.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/artillery	Block	1
195.154.226.90	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
114.134.186.241	Cambodia	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
77.125.129.197	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/maslulim/	Block	1
207.46.13.144	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
157.55.39.238	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/history/in_mivzaim.asp	Block	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
31.210.189.252	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
97.100.214.210	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
66.249.66.31	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/givati/	Block	1
195.154.226.90	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
114.134.186.241	Cambodia	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kap@z/	Block	1
79.177.132.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
14.33.86.45	Korea, Republic of	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.66.75	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.75	Block	1
31.210.189.252	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
97.100.214.210	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
66.249.75.94	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/general.aspx	Block	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
195.154.226.90	France	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 195.154.226.90	Block	1
124.73.7.208	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1328-he/cogat.aspx/trackback/	Block	1