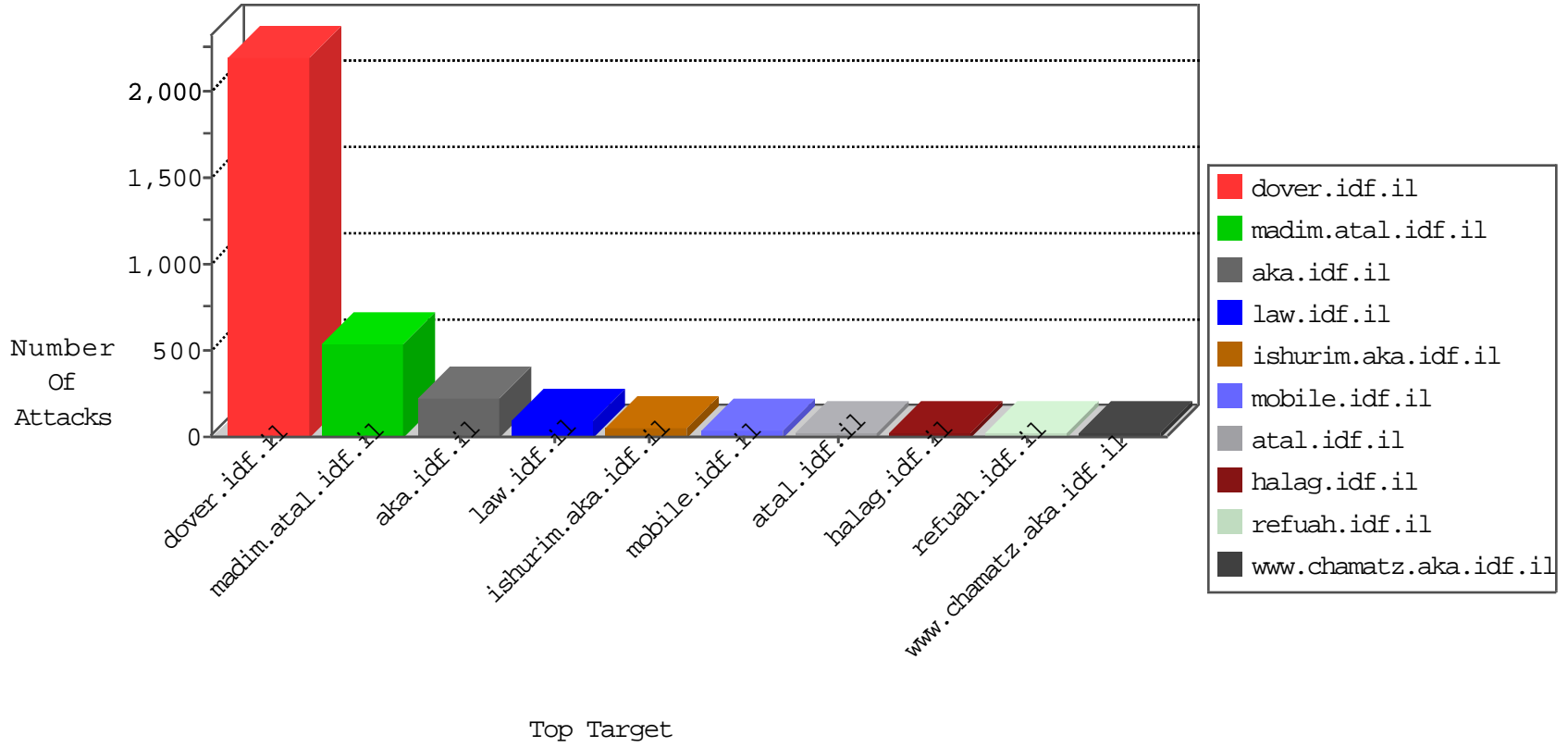


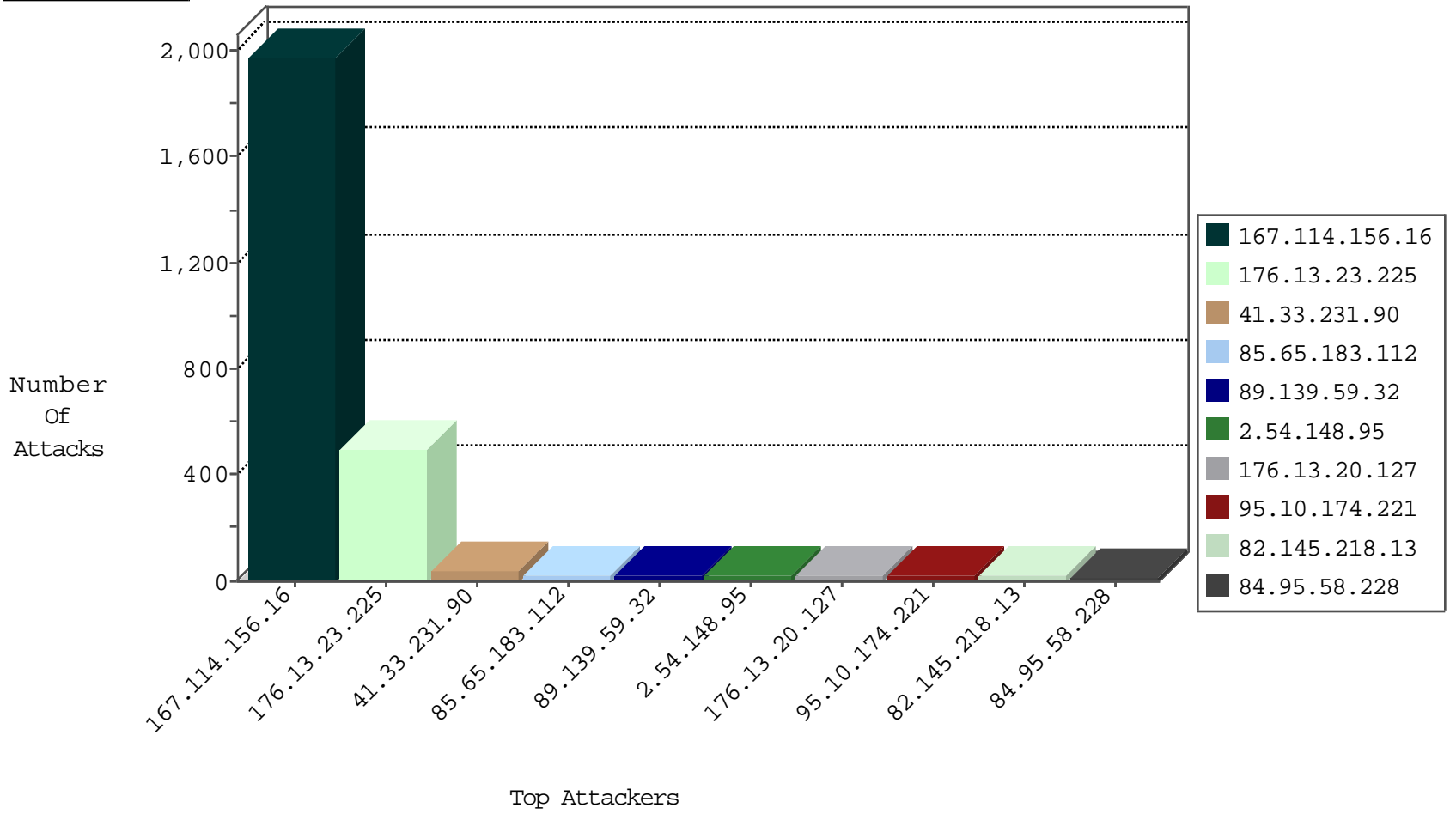
IDF Under Attack Daily Report



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	3098
107.170.42.128	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
204.42.253.2	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-trafl	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.10.174.221	Turkey	147.237.77.74	law.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
95.10.174.221	Turkey	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
62.210.162.217	France	147.237.77.216	dover.idf.il	19791: HTTP: WordPress N-Media PHP File Upload	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
95.10.174.221	147.237.77.74	Turkey	law.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	12
95.10.174.221	147.237.77.216	Turkey	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
31.168.181.151	147.237.76.42	Israel	refuah.idf.il	ET SCAN NMAP -sA (2)	2
66.249.81.212	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
176.60.66.183	147.237.76.177	Belarus	noore.idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
176.60.66.183	147.237.0.200	Belarus	m4u.idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
176.13.20.127	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
94.102.48.195	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
202.124.48.157	147.237.77.227	Japan	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
82.80.132.84	147.237.76.30	Israel	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
202.124.48.157	147.237.77.227	Japan	e.hamaz.idf.il	ET SCAN NMAP -f -sS	1
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
62.232.207.210	147.237.0.34	United Kingdom	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
176.60.66.183	147.237.77.176	Belarus	matpash.idf.il	ET SCAN Potential SSH Scan	1
62.232.207.210	147.237.0.15	United Kingdom	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
176.60.66.183	147.237.8.14	Belarus	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
176.60.66.183	147.237.0.16	Belarus	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
112.16.76.209	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
218.104.49.211	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
202.124.48.157	147.237.77.227	Japan	e.hamaz.idf.il	ET SCAN NMAP -sS window 2048	1
195.154.154.131	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
62.232.207.210	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN Potential SSH Scan	1
176.60.66.183	147.237.77.226	Belarus	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
62.232.207.210	147.237.0.16	United Kingdom	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	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
89.139.59.32	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
82.145.218.13	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
79.177.164.172	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
185.89.217.225		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	14
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
87.68.153.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.148.164	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.181.0.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.148.95	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
176.13.20.127	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
80.246.136.23	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.67.118.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.65.183.112	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
84.95.58.228	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	8
84.95.58.228	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.13.20.127	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
84.111.32.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	7
94.230.86.190	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.89.217.230		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.234		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.231		147.237.77.74	law.idf.il	drop	First packet isn't SYN	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
185.89.217.232		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.235		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.138	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.89.217.227		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
79.180.165.64	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
31.154.146.42	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
31.154.146.42	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
212.150.97.238	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
31.154.146.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
185.89.217.229		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.65.183.112	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.226		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
46.117.74.18	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
85.65.183.112	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
185.89.217.227		147.237.77.74	law.idf.il	drop		drop	4
46.117.74.18	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
91.200.12.143	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
85.65.183.112	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
157.55.39.178	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.117.74.18	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.23.225	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.23.225	Block	263
176.13.23.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	195
176.13.23.225	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.13.23.225	Block	43
185.27.105.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
62.210.162.217	France	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	7
62.210.162.217	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 62.210.162.217	Block	6
2.54.63.55	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	4
37.26.148.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.219.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.128.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.168.6.66	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/7/109097.pdf	Block	2
176.13.7.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.77.49.236	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
185.32.179.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
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	2
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	2
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/misrot.aspx	Block	1
2.54.158.226	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/1133-22638-he/dover.aspx.	Block	1
84.228.224.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.121.137.42	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
207.46.13.150	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 207.46.13.150	Block	1
37.142.184.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.49.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.131	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
5.101.156.63	Russian Federation	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
128.232.110.29	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
52.91.234.90	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
213.57.164.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.24.134	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
89.139.59.32	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.182.167.112	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.99.160.171	Canada	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
69.194.230.99	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
37.26.148.233	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.4.72	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.88.18	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.37.160	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
65.19.167.130	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
50.62.161.42	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
40.77.167.27	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/captcha.ashx	Block	1
79.179.37.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.86	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/shared/usercontrols/headerupper/	Block	1
141.212.121.176	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
52.91.234.90	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1