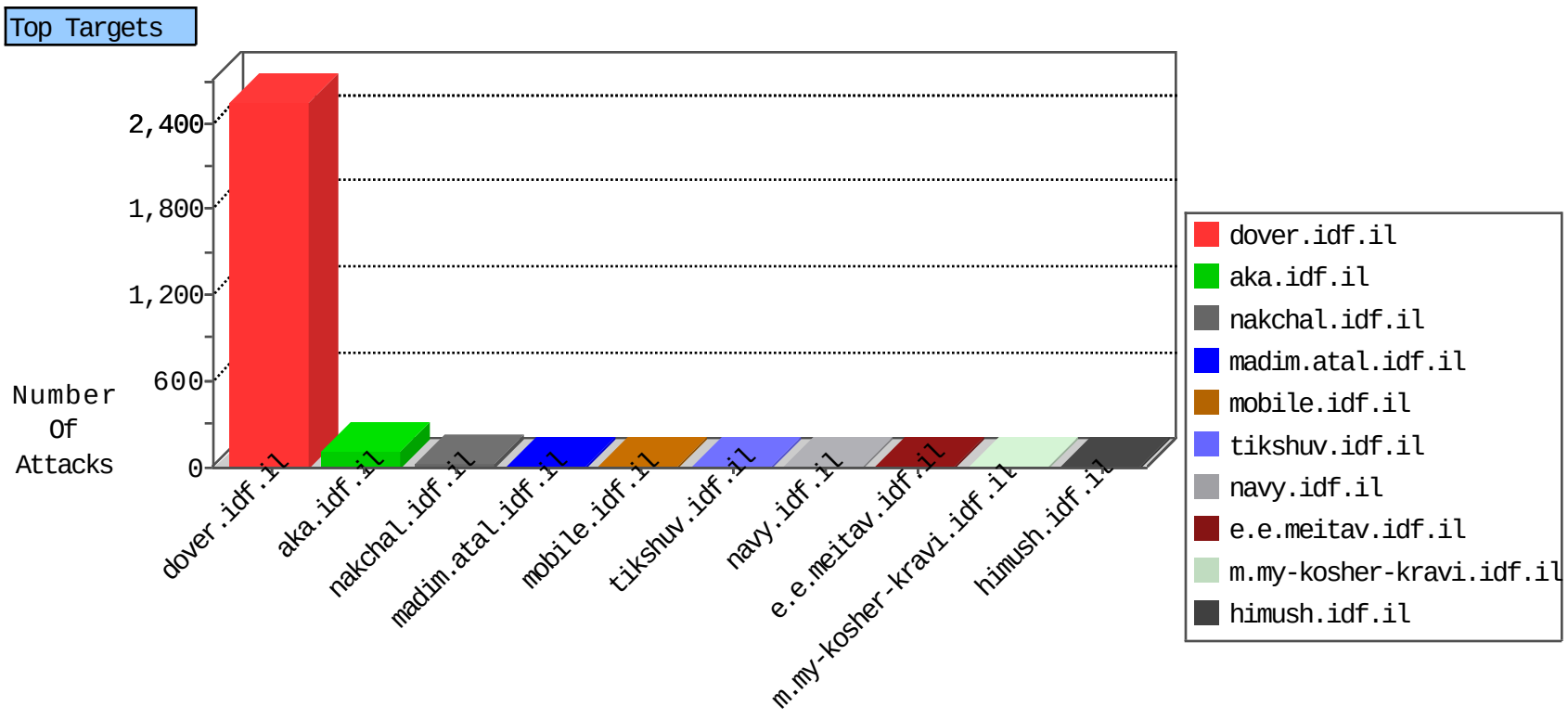
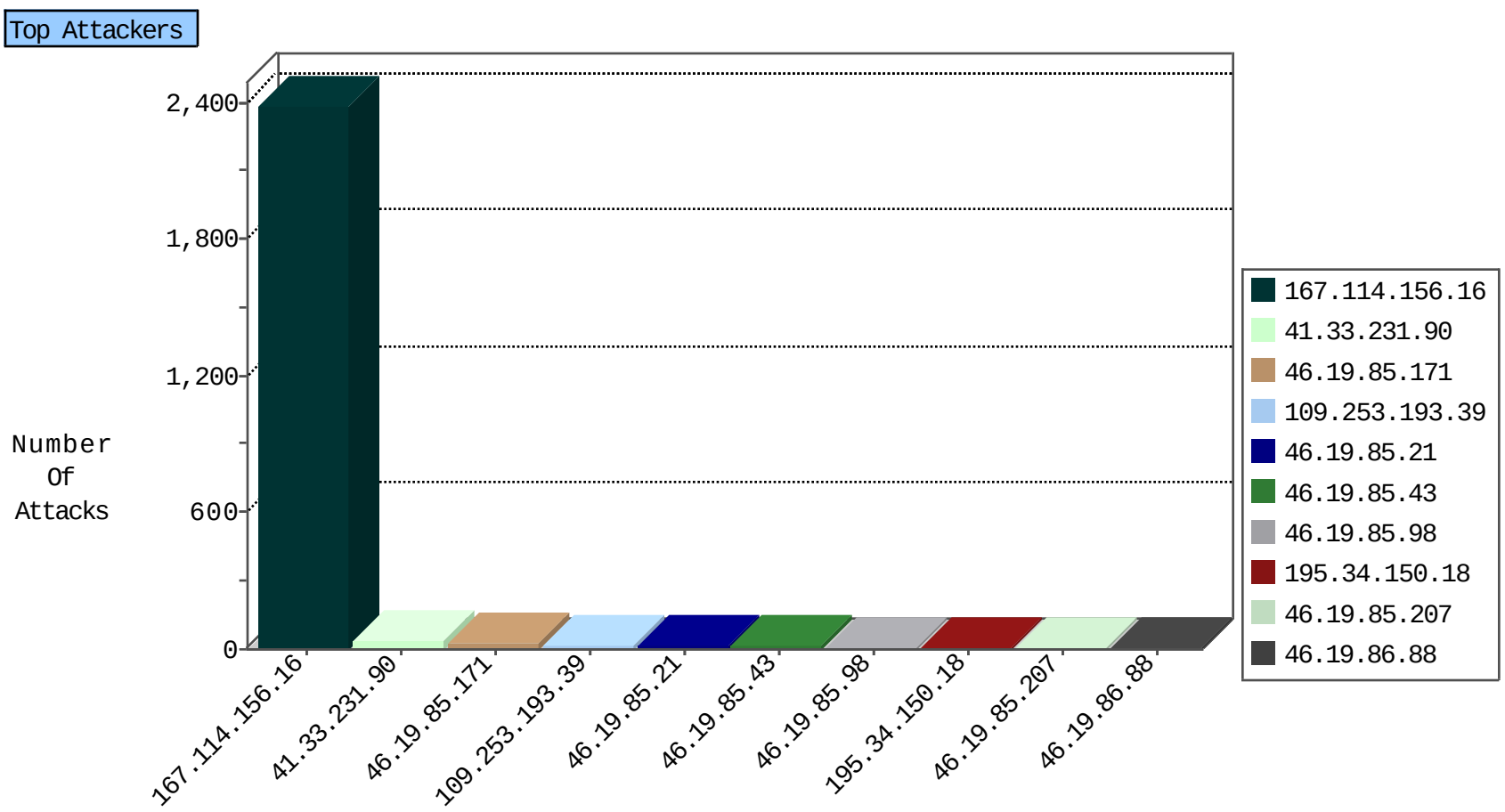
12-22-2015-07:04:00 to 12-22-2015-08:04:00

IDF Under Attack Daily Report





Top Attackers

12-22-2015-07:04:00 to 12-22-2015-08:04:00

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	3267
113.128.147.21	China	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
115.239.228.10	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Http	drop	2
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
220.208.49.66	Japan	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
61.24.220.110	Japan	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
71.6.135.131	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
140.224.63.138	China	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1

12-22-2015-07:04:00 to 12-22-2015-08:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-22-2015-07:04:00 to 12-22-2015-08:04:00

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
66.249.81.239	147.237.72.167	United States	ishurim.aka.idf.i	ET SCAN NMAP -sA (2)	2
195.22.126.20	147.237.0.34	Poland	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
183.61.109.189	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
134.213.133.4	147.237.72.217	United Kingdom	e.idf.il	ET SCAN NMAP -sS window 4096	1
134.213.133.4	147.237.72.217	United Kingdom	e.idf.il	ET SCAN NMAP -f -sS	1
94.159.177.30	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.208	147.237.72.217		e.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.162	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
134.213.133.4	147.237.72.217	United Kingdom	e.idf.il	ET SCAN NMAP -sS window 2048	1
101.108.189.19	147.237.0.35	Thailand	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
211.140.232.91	147.237.0.200	China	m4u.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1

12-22-2015-07:04:00 to 12-22-2015-08:04:00

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
46.19.85.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
109.253.193.39	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
46.19.85.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.120.167.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.88	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.21	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.207	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.228.62.213	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	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
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.207	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.54.46.52	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.21	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.22.131.93	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.127.240.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.218.193	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
207.46.13.152	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.134.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.0.81.57	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
109.66.39.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
50.18.94.121	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
31.168.164.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.88	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.54.32.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
192.0.80.167	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
46.120.91.125	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.32.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.175	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.57.203.53	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
208.115.113.89	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
2.54.32.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
46.19.85.21	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.218.206.70	United States	147.237.8.24	e.lifestyle.idf	Geo-location enforcement	Geo-location inbound enforcement	drop	1
31.168.164.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
208.115.113.89	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
2.52.181.90	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.32.179.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
46.19.85.149	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.143	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
45.33.61.138		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
82.80.210.133	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
212.235.98.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
82.81.2.165	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	4
199.16.156.124	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/5/size220x0/17765.jpg	Block	4
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	4
176.13.8.151	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	3
46.19.85.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.117.164.60	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 46.117.164.60	None	3
2.54.46.52	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
79.179.183.139	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.179.183.139	Block	3
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
79.181.151.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
207.46.13.1	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
199.59.148.210	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/5/size220x0/17765.jpg	Block	2
109.253.215.76	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
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	2
84.94.38.200	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	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
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
37.26.148.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
110.168.186.130	Thailand	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
84.109.69.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/include/vdimgck.php	Block	1
199.30.25.146	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.183.139	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
158.130.0.242	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.117.164.60	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
2.54.25.242	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.8.245.50	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/searchback.png	Block	1
109.67.57.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.80	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
176.13.8.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
119.94.188.203	Philippines	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
89.138.209.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.65	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
199.59.148.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/5/size220x0/17765.jpg	Block	1
176.12.139.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.34.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.151.35.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.163.234.9	Romania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
119.94.188.203	Philippines	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
46.19.86.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.80	United States	147.237.72.166	aka.idf.il	Unknown Parameter </script in www.aka.idf.il/ishurim/main/url	None	1
79.183.106.80	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.120.167.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.5.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.43.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.81.2.165	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	1