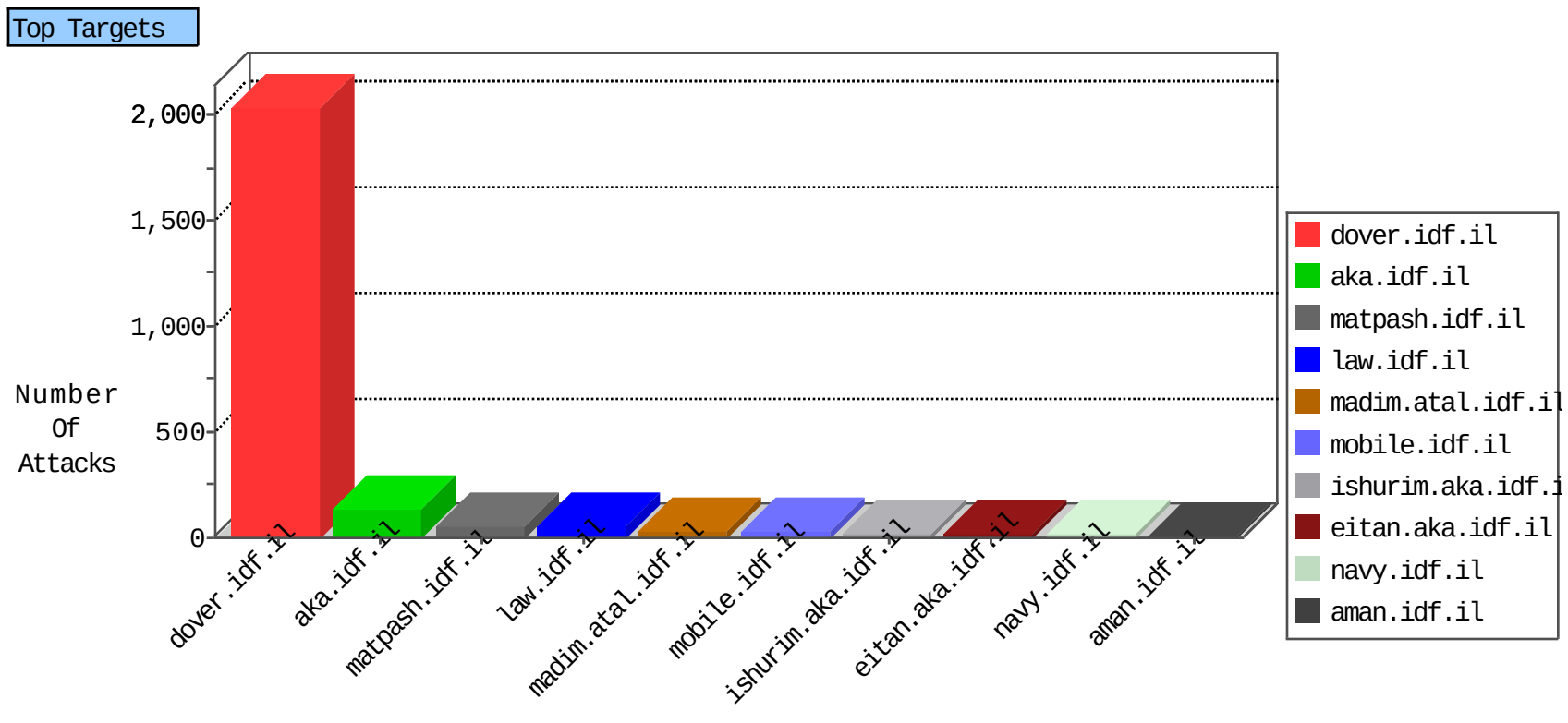
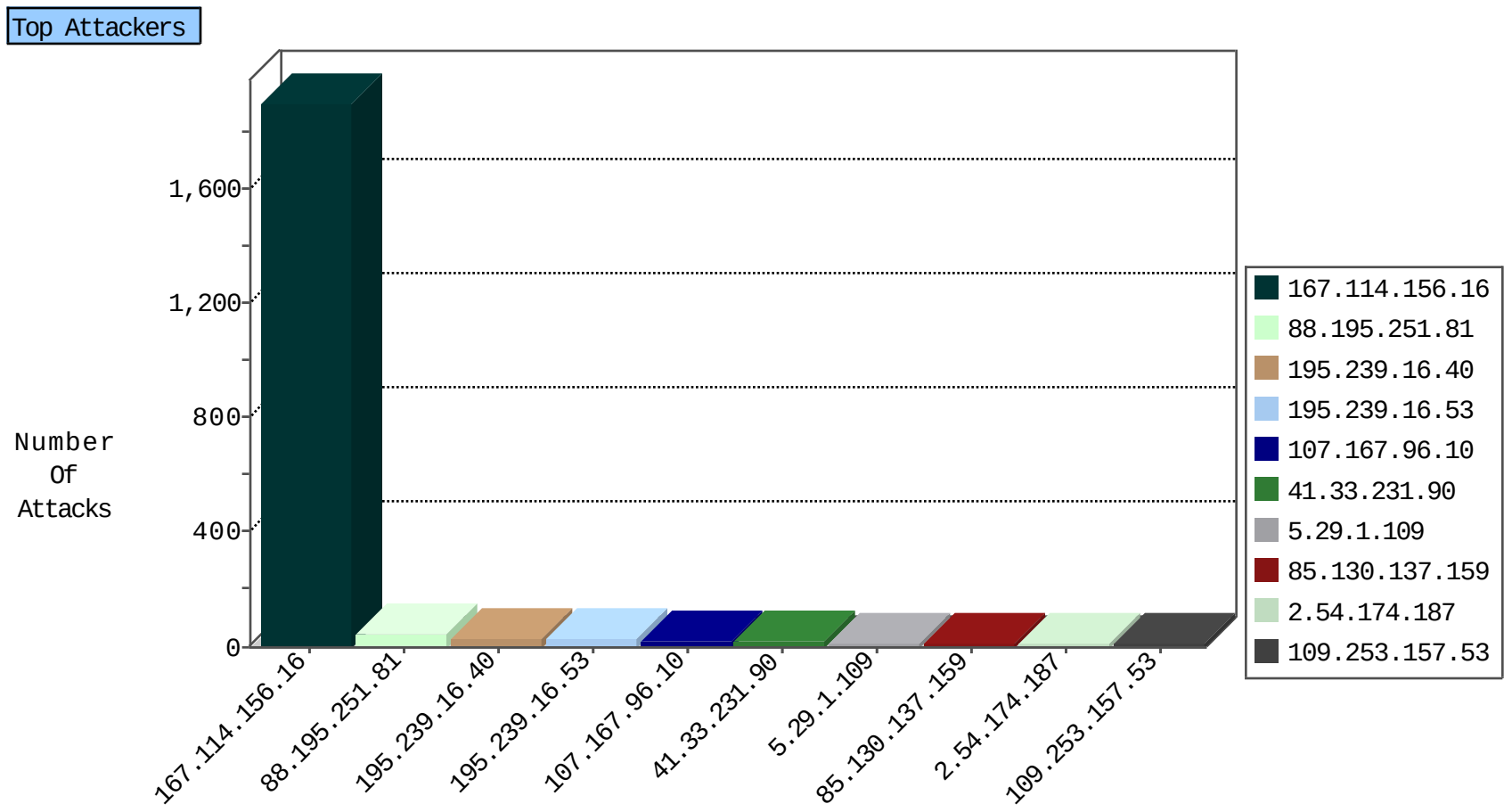
01-21-2016-23:04:09 to 01-22-2016-00:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-21-2016-23:04:09 to 01-22-2016-00:04:09

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	3053
91.193.140.76	Russian Federation	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
200.35.95.235	Venezuela	147.237.72.167	ishurim.aka.idf.il	L4 Source or Dest Port Zero	drop	1
89.46.102.242	Romania	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
91.193.140.76	Russian Federation	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
91.193.140.76	Russian Federation	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
162.248.100.195	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
91.193.140.76	Russian Federation	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

01-21-2016-23:04:09 to 01-22-2016-00:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.236.51.169	United Kingdom	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	2
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

01-21-2016-23:04:09 to 01-22-2016-00:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
104.192.0.226	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
95.154.201.156	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.82.79.104	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
213.151.55.110	147.237.77.216	Israel	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
190.249.184.162	147.237.77.178	Colombia	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
190.249.184.162	147.237.77.178	Colombia	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
108.168.185.133	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
95.154.201.156	147.237.0.19	United Kingdom	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.169.86	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
80.82.79.104	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
190.249.184.162	147.237.77.178	Colombia	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
178.19.155.126	147.237.77.216	Italy	dover.idf.il	ET SCAN NMAP -sS window 4096	1

01-21-2016-23:04:09 to 01-22-2016-00:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
88.195.251.81	Finland	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	48
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
107.167.96.10	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
2.54.174.187	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.22.1	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
46.19.86.172	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
109.253.157.53	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
188.120.148.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.29.1.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
5.29.1.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
66.249.78.252	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.137.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.137.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
31.210.187.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.130.137.159	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
31.210.187.171	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.131.66	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.136.62	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	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
46.121.123.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.99.32.2		147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.233.151	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.178.138.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.134.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.120.102.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.3.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.14.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.117.50.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.131.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.135.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.56.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.162.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.163.171	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.176.132.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.129.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.180.125.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.246.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.59.253	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.66.131.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.212.121.192	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
109.253.218.217	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
195.239.16.40	Russian Federation	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.65.99.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
185.32.179.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.160.165.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.1.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.253.157.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.171.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.57.157.172	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
84.108.81.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.120.207.175	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
161.0.110.127	Netherlands Antilles	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
5.22.131.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.68.62.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1
146.185.234.48	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
37.142.239.132	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.7.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
103.16.228.98	Hong Kong	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
84.228.247.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.148.26.78	Lithuania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
173.252.90.125	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.134.44	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/milluim/index	Block	1
89.139.133.111	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &SortDir in www.eitan.aka.idf.il/1104-he/eitan.aspx	None	1
149.78.174.204	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.242.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.8.127	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
104.128.144.131	Canada	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
84.229.39.223	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
60.53.27.128	Malaysia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
176.13.1.75	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.100.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.187.144.122	Czech Republic	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
207.46.13.122	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/1551-he/images/shared/err_page.png	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1117-he/nakhal.aspx	Block	1
157.55.39.194	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
46.19.85.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
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	1
60.53.27.128	Malaysia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
176.13.3.48	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.253.157.53	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
8.37.233.162	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.121.31	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/&sa=u&ved=0ahukewj4-vtm6bvkahvbthqkhfluajkqfggumam&usg=afqjcnhcvyyg7w1cq-yhd5_ammzoyodtwa	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
80.246.137.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
161.0.110.127	Netherlands Antilles	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
46.19.86.84	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.171.128	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
85.65.191.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1