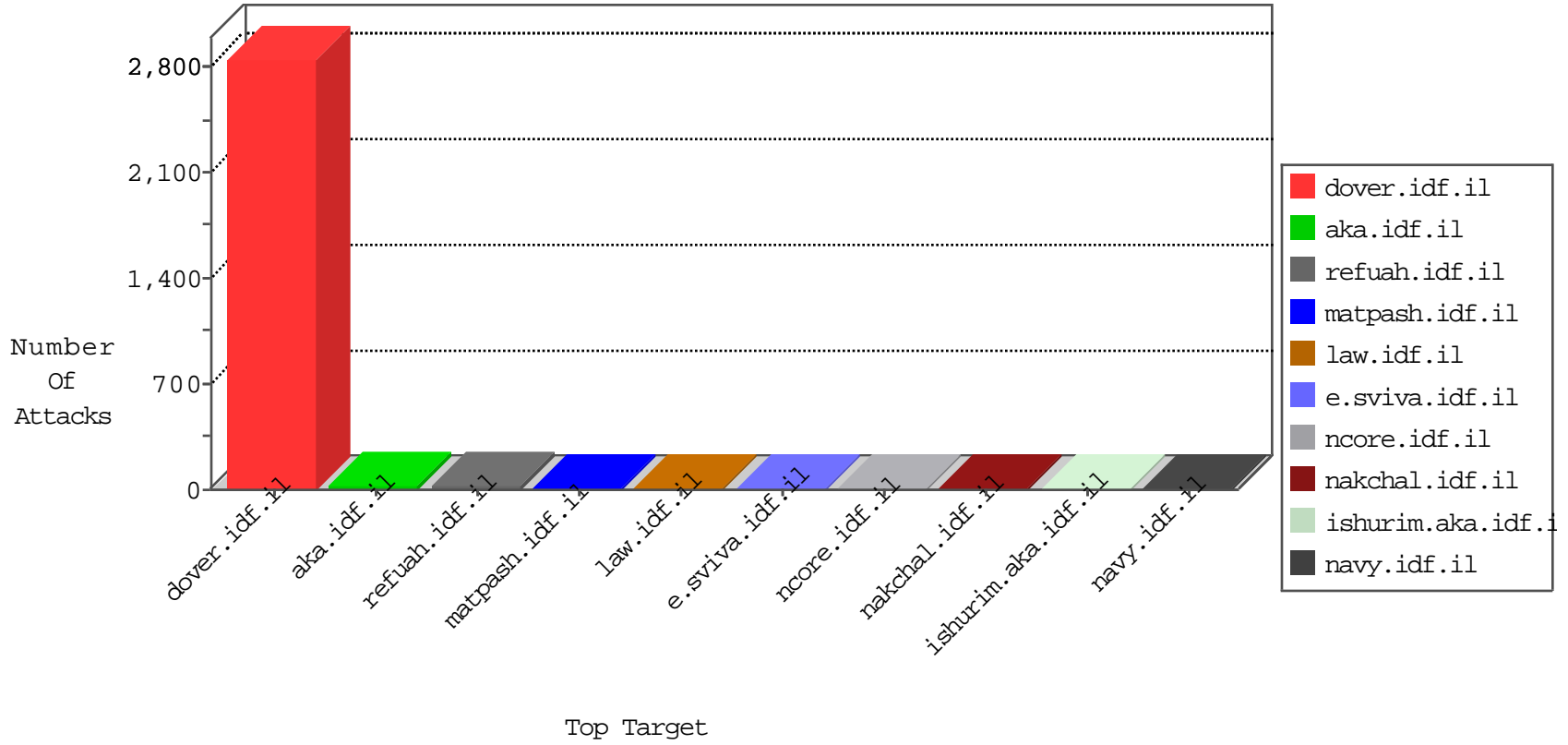


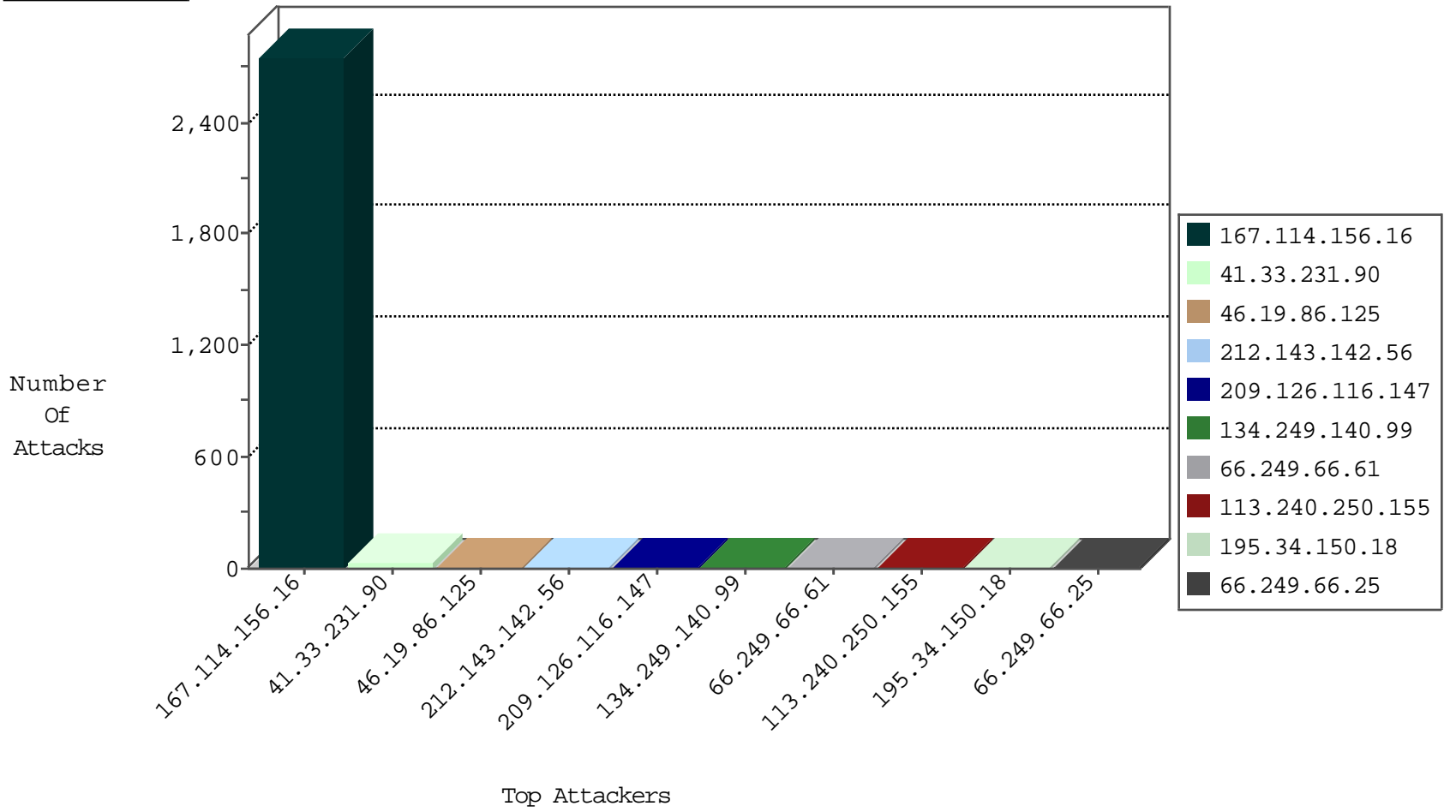
IDF Under Attack Daily Report



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	3566
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.132	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
54.67.60.7	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.117	France	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	1
198.20.69.74	United States	147.237.77.179	e.mazi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
69.12.70.34	United States	147.237.77.176	matpash.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
167.114.242.197	Canada	147.237.76.31	nakchal.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	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
113.240.250.155	147.237.76.177	China	ncore.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
66.249.66.25	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
216.215.12.72	147.237.76.30	United States	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
193.105.134.220	147.237.76.38	Sweden	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.67.224	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
62.212.73.196	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
41.253.8.82	147.237.8.28	Libyan Arab Jamahiriya	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
180.153.104.125	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
113.240.250.155	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
46.151.55.35	147.237.77.61	Ukraine	e.cogat.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	26
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.125	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.125	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
82.44.203.232	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
153.92.127.143	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
66.249.66.1	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
185.100.85.101		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
193.90.12.86	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
209.126.116.147	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
46.246.124.92	Sweden	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	1
194.150.168.95	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
153.92.126.135	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
113.240.250.155	China	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
71.6.165.200	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
209.126.116.147	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
184.105.247.240	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.71	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.10.210.199	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
46.246.124.92	Sweden	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
195.62.53.168	Russian Federation	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
119.94.218.44	Philippines	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.10	United States	147.237.0.33	idf.il	drop		drop	1
209.126.116.147	United States	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
46.117.81.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.3.146.207	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
146.185.239.102	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.93.18.64	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
216.218.206.74	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
198.20.69.74	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.180	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.11	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
209.126.116.147	United States	147.237.76.39	mobile.meitav.idf.il	drop	SAM rule	drop	1
46.166.170.6	Lithuania	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
146.185.239.102	Russian Federation	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
89.31.57.5	Italy	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
202.112.51.96	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
172.56.17.0	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.181	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.32	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
209.126.116.147	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.246.124.92	Sweden	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.187.129.166	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
94.102.48.195	Netherlands	147.237.0.35	akaws.idf.il	drop		drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.128.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.81	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.81	Block	2
134.249.140.99	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 134.249.140.99	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
37.26.147.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/*x*s*x*x* 7	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
134.249.140.99	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
54.153.33.145	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
103.16.69.14	India	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9014-he/refuah.aspx	Block	1
157.55.39.186	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.aspx	None	1
41.69.251.43	Egypt	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
86.124.62.18	Romania	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	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
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation pageNum in www.idf.il/1393-en/dover.aspx	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
41.69.251.43	Egypt	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
119.94.218.44	Philippines	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
86.124.62.18	Romania	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
66.249.67.133	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/2330.jpg	Block	1
134.249.140.99	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/blog/	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation pageNum in www.idf.il/1841-he/dover.aspx	Block	1
66.249.66.69	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/19102010masaiyot.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
46.117.81.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
119.94.218.44	Philippines	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
89.31.57.5	Italy	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
66.249.67.224	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
141.212.122.64	United States	147.237.72.167	ishurim.aka.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-16973-he/dover.aspx	Block	1
40.77.167.78	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	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
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.75	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.75	Block	1
207.46.13.154	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19748-he/idfgdover.aspx	Block	1
134.249.140.99	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.120.156.245	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
103.16.69.14	India	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.67.243	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluuml/templates/main.asp	Block	1
157.55.39.17	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16602-en/dover	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
40.77.167.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	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
74.6.53.166	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1