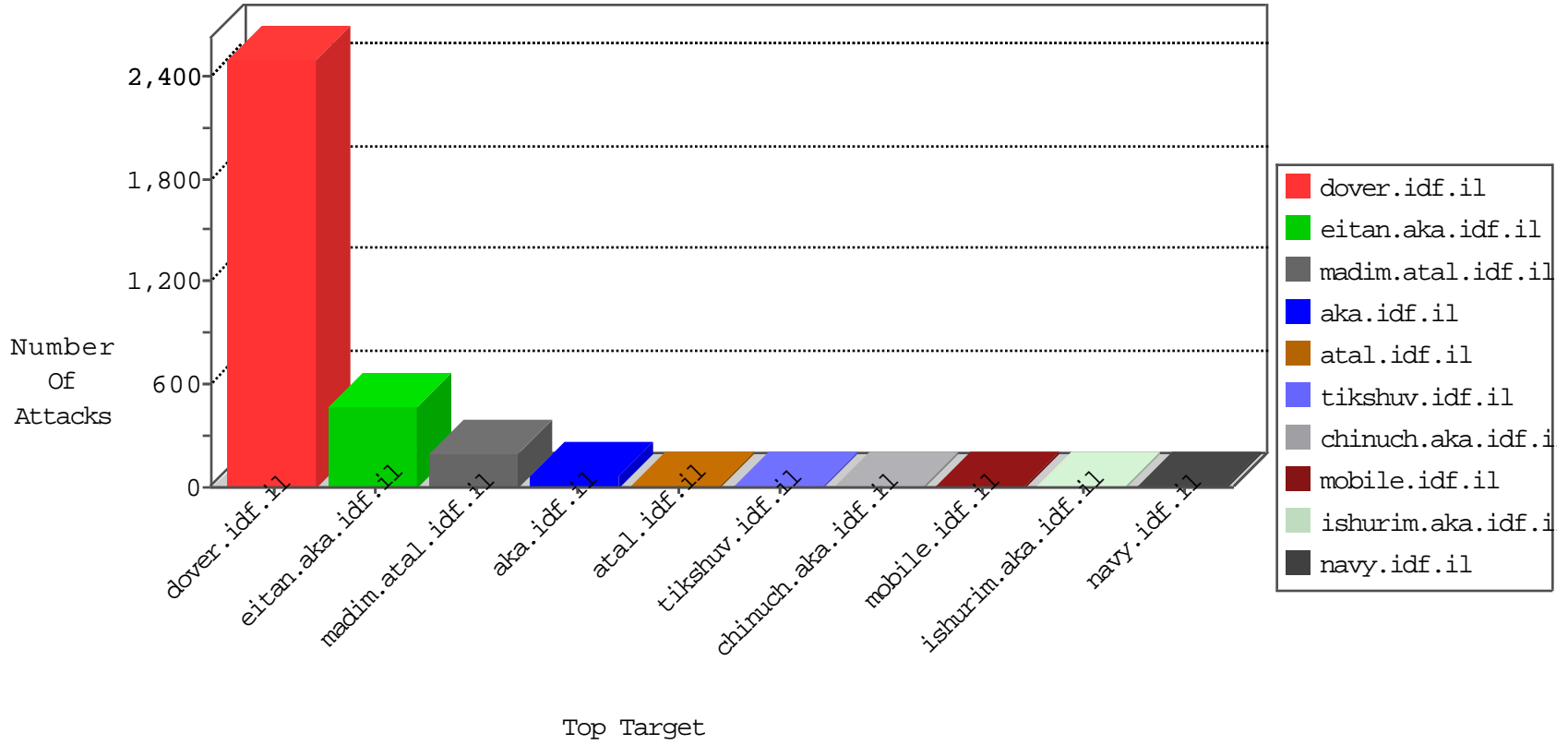


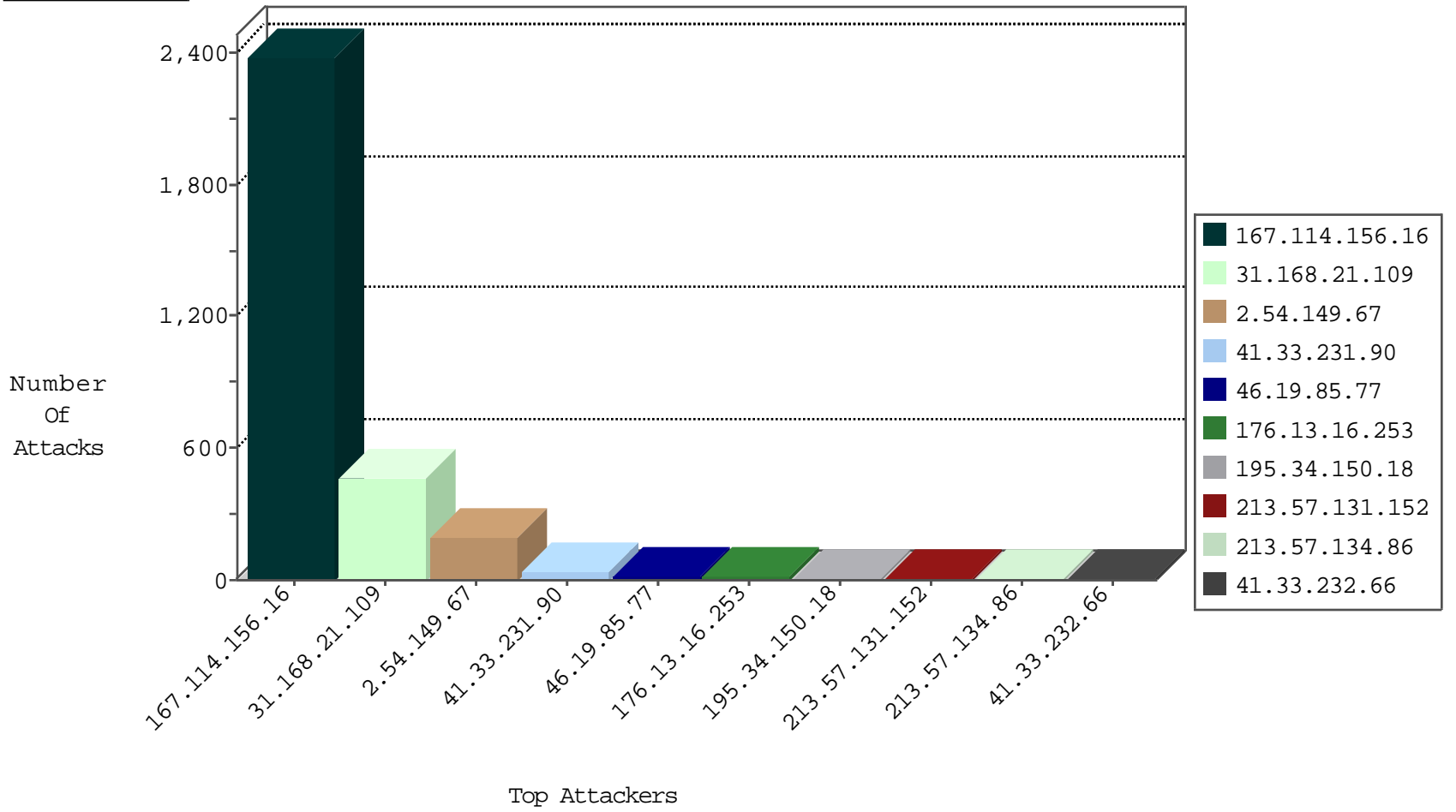
IDF Under Attack Daily Report



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	3490
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1

12-21-2015-01:07:51 to 12-21-2015-02:07:51

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.46.13.160	United States	147.237.77.216	dover.idf.il	C076: HTTP: Access to - action=... (General)	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
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
46.148.16.98	147.237.76.197	Lithuania	e.himush.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.2	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
46.148.16.98	147.237.76.30	Lithuania	himush.idf.il	ET SCAN Potential SSH Scan	1
94.102.60.89	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
37.143.82.50	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
83.110.99.208	147.237.76.86	United Arab Emirates	navy.idf.il	ET SCAN NMAP -sS window 3072	1
37.143.82.50	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
83.110.99.208	147.237.76.86	United Arab Emirates	navy.idf.il	ET SCAN NMAP -f -sS	1
67.192.247.232	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
67.192.247.232	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.77.216	Cote D'Ivoire	dover.idf.il	ET SCAN NMAP -sS window 4096	1
46.148.16.98	147.237.76.201	Lithuania	e.atal.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.2	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.148.16.98	147.237.76.147	Lithuania	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
125.27.19.180	147.237.8.28	Thailand	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.148.16.98	147.237.0.19	Lithuania	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.162	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Rapid IMAP Connections - Possible Brute Force Attack	1
37.143.82.50	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
83.110.99.208	147.237.76.86	United Arab Emirates	navy.idf.il	ET SCAN NMAP -sS window 2048	1
67.192.247.232	147.237.76.86	United States	navy.idf.il	ET SCAN Potential SSH Scan	1
67.192.247.232	147.237.72.156	United States	aman.idf.il	ET SCAN Potential SSH Scan	1
201.7.213.4	147.237.77.216	Brazil	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
67.192.247.232	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.77.216	Cote D'Ivoire	dover.idf.il	ET SCAN NMAP -sS window 1024	1
46.148.16.98	147.237.77.216	Lithuania	dover.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.76.34	United States	yohalan.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
31.168.21.109	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	426
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.85.77	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
176.13.16.253	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.131.152	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
176.13.16.253	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
213.57.134.86	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.20.136	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
93.173.236.124	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
185.3.144.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.147.156	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
157.55.39.45	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.28.81	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
77.125.132.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.5.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.212.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.50.14	Russian Federation	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.159.145.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.152.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.57.134.86	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
185.3.146.101	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.57.131.152	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
46.19.86.50	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.46.34.135	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
176.13.20.136	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
213.57.132.99	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
109.65.152.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
107.150.43.203	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.51	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	1
139.196.104.39	China	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
107.150.43.204	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
46.19.86.78	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.26.147.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
115.230.124.164	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.88.157.67	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.120.216.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.3.146.218	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.50	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	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
155.94.222.12	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.64.212.64	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
185.120.126.35		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.149.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	100
2.54.149.67	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.149.67	Block	95
31.168.21.109	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 31.168.21.109	Block	37
46.19.86.58	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.194	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
109.65.152.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.69.8	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	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
79.179.134.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/gyus/general.aspx	Block	1
31.154.135.243	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
89.138.51.22	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	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
207.46.13.138	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
2.54.14.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
86.127.72.53	Romania	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1361-10641-he/dover.aspx	Block	1
31.168.21.109	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.32.179.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
104.232.3.33		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.166.190.139	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
109.201.154.173	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
86.127.72.53	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
185.100.84.82		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
31.168.21.109	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	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
72.68.228.52	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
116.75.1.244	India	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
89.38.150.47	Romania	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
31.168.21.109	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	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
74.7.105.230	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
23.106.26.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22197-ar/dover.aspx)	Block	1
116.75.1.244	India	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
89.38.150.47	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-signup.php	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/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
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