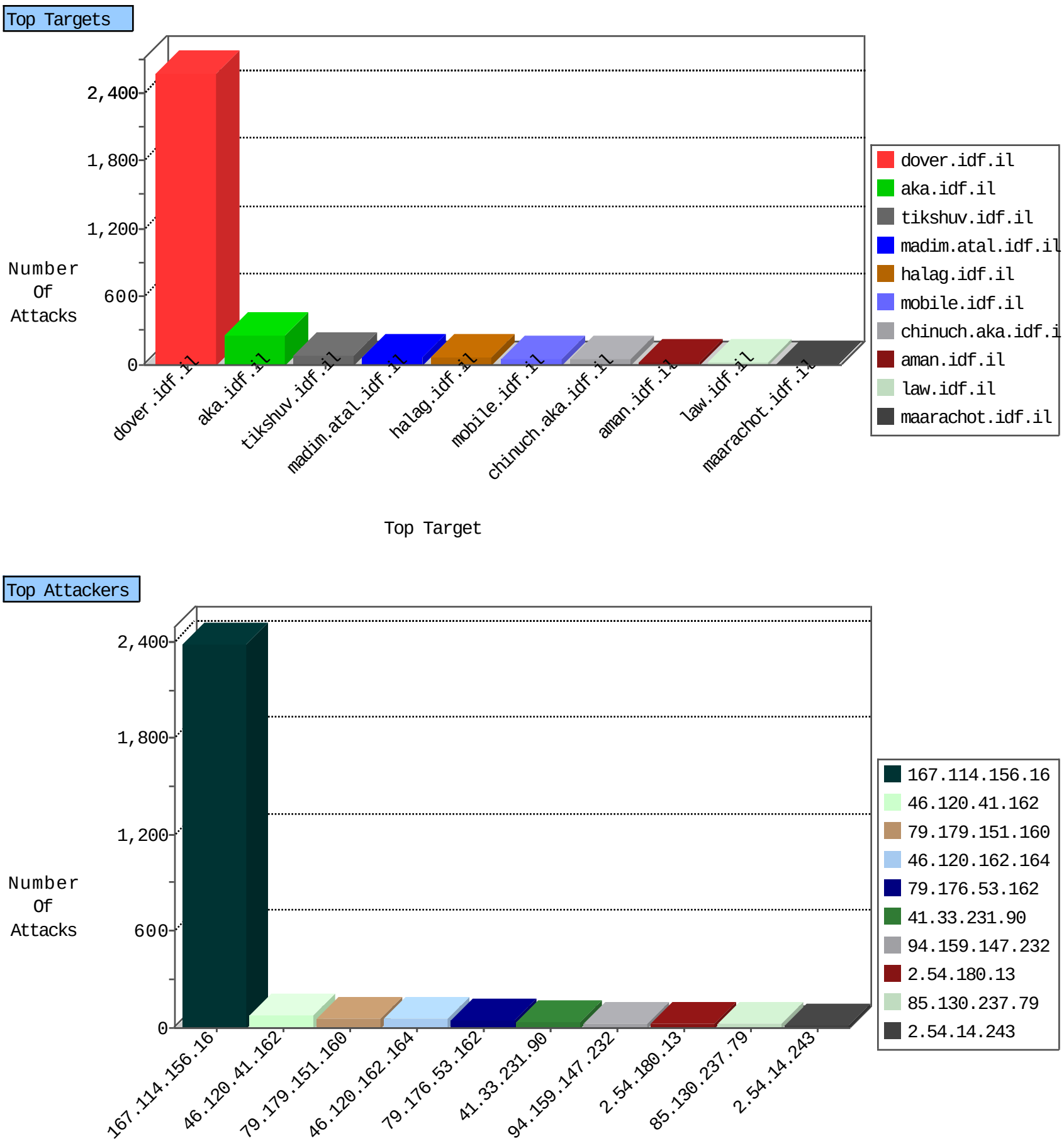
01-23-2016-21:04:09 to 01-23-2016-22:04:09

IDF Under Attack Daily Report



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

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	3107
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	170
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.97.48	France	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1
172.245.218.130	United States	147.237.77.216	dover.idf.il	0543: HTTP: php.cgi Access	Block	1
188.165.15.44	France	147.237.76.147	chinuch.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1

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

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
66.249.78.111	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
195.216.176.244	147.237.8.50	Latvia	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
131.109.15.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
131.109.15.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -f -sS	1
114.112.90.54	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.130.24	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
37.142.137.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
131.109.15.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
118.174.192.200	147.237.76.30	Thailand	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.174.93.181	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
23.101.3.156	147.237.0.17	Hong Kong	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.120.162.164	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	53
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
79.179.151.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
94.159.147.232	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
94.159.147.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
2.54.14.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.185.255	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
157.55.39.114	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.46.39.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.157.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.250.251.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.3.147.187	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
109.67.104.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.237.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.172.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.58.110	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.168	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	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
79.182.172.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.250.251.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.28.150.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.237.79	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
31.25.72.89	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
85.130.237.79	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
94.230.86.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.39.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.131.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.25.72.89	Palestinian Territory, Occupied	147.237.77.216	dover.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
31.168.245.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
208.52.161.99	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
79.180.126.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.58.10	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.183.179.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.188.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.158.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.8.173.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.209.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.28.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.94.123.195	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
2.54.159.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.239.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.76.127.10	Israel	147.237.77.234	halag.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3

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

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
5.28.144.240	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
5.22.131.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.41.162	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 46.120.41.162	Block	70
2.54.180.13	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
77.126.220.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
79.178.137.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
85.250.215.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
46.19.86.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
176.13.15.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.14.243	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.54.157.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
172.245.218.130	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 172.245.218.130	Block	3
37.46.42.60	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
95.86.101.153	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.86.101.153	Block	3
46.19.85.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.179.151.160	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 79.179.151.160	Block	2
37.142.189.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.179.151.160	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 79.179.151.160	Block	2
79.179.151.160	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 79.179.151.160	Block	2
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	2
79.179.151.160	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 79.179.151.160	Block	2
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-8321-he/dover.aspx	Block	1
79.183.124.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.151.160	Israel	147.237.72.166	aka.idf.il	Too Many Headers per Request - 35 Headers	Block	1
62.114.224.180	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
109.253.196.86	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
79.179.151.160	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 79.179.151.160	Block	1
5.22.129.143	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	1
87.69.243.125	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.69.49	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/1/106911.pdf	Block	1
149.88.217.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.96.48	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
46.120.162.164	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
109.67.28.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.151.160	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 79.179.151.160	Block	1
79.179.151.160	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL tl[[#3]]x9gÂ¢×³×€Â-Â c	Block	1
212.76.101.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.137.128	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.101.153	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1361-10628-he/dover.aspx&sa=u&ved=0ahukewidnnsb08dkahugdcwkhvq1dgeqfggjmaq&usg=afqjcnf9pf0i4fsibbilbo_vah3iio6drg	Block	1
2.54.58.110	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
85.93.91.84	Germany	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/templates/	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
185.3.147.187	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.179.151.160	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
62.114.224.180	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
128.71.53.86	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
5.22.129.143	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	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

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