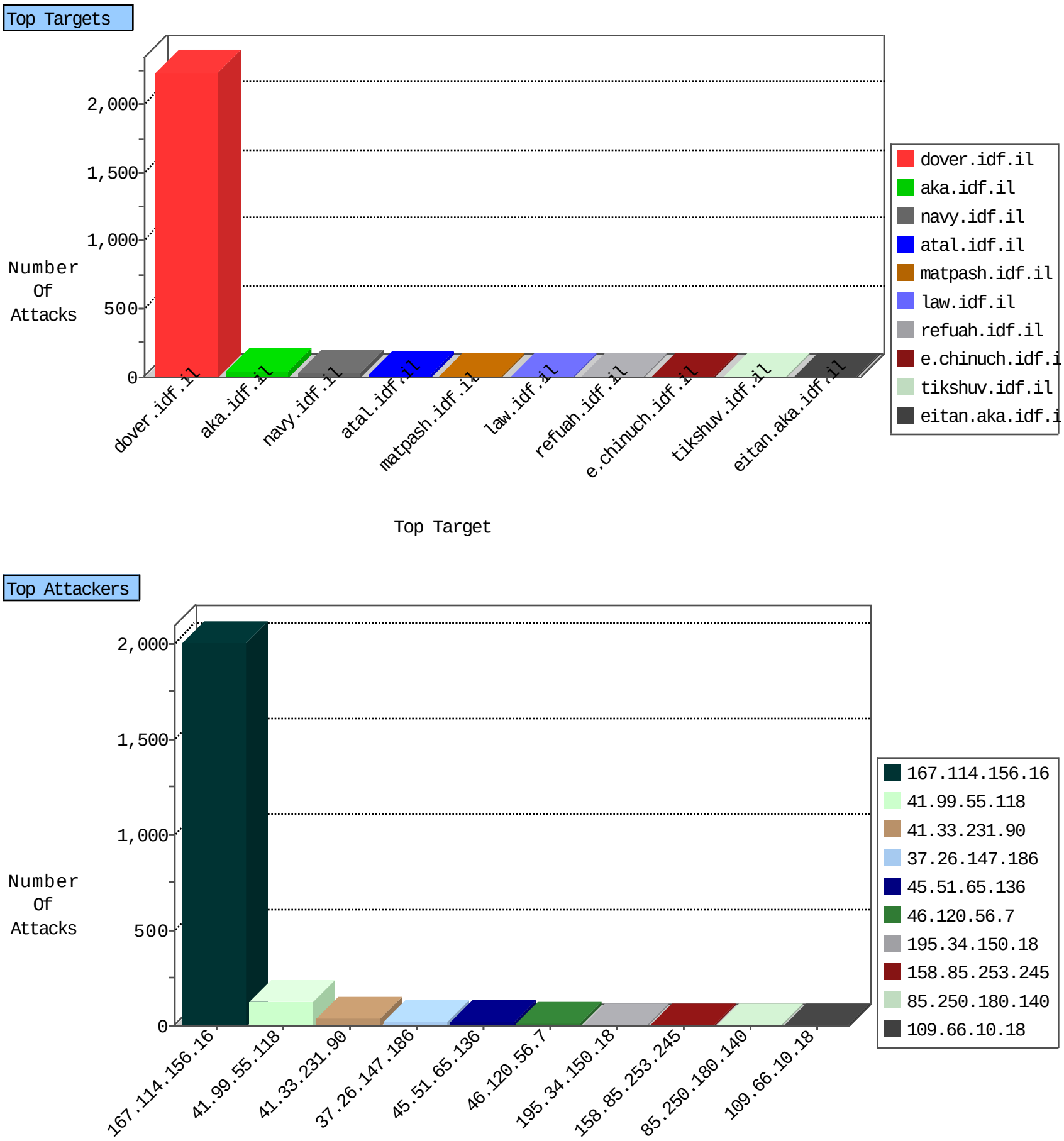
01-22-2016-02:04:04 to 01-22-2016-03:04:04

IDF Under Attack Daily Report



01-22-2016-02:04:04 to 01-22-2016-03:04:04

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	3027
41.99.55.118	Algeria	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	907
41.99.55.118	Algeria	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	19
181.113.122.70	Ecuador	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
200.35.95.235	Venezuela	147.237.0.200	m4u.idf.il	L4 Source or Dest Port Zero	drop	1
175.12.5.33	China	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
181.113.122.70	Ecuador	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
94.102.51.38	Netherlands	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

01-22-2016-02:04:04 to 01-22-2016-03:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.99.55.118	Algeria	147.237.77.216	dover.idf.il	10767: HTTP: Acunetix Security Scanner	Block	2
41.99.55.118	Algeria	147.237.77.216	dover.idf.il	3999: HTTP: Cross Site Scripting Attack in HTTP Header	Block	2
144.76.4.148	Germany	147.237.76.86	navy.idf.il	C106: HTTP: majestic bot	Block	1
87.106.179.116	Germany	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
89.19.29.90	Turkey	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

01-22-2016-02:04:04 to 01-22-2016-03:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
158.85.253.245	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
89.19.29.90	147.237.77.233	Turkey	atal.idf.il	SQL Injection - Select From	3
87.106.179.116	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	3
66.249.78.159	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
119.30.47.130	147.237.76.86	Bangladesh	navy.idf.il	ET SCAN NMAP -sA (2)	2
91.201.236.113	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
220.132.33.10	147.237.8.28	Taiwan	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
184.190.30.34	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
85.93.5.66	147.237.76.147	Germany	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
173.203.64.151	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
41.99.55.118	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP server-info access	1
172.98.200.238	147.237.8.46		e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
223.4.174.30	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
119.81.188.158	147.237.77.233	Hong Kong	atal.idf.il	ET SCAN NMAP -sS window 1024	1
223.4.174.30	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
101.109.150.145	147.237.76.30	Thailand	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
221.131.184.209	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.77.216	Ukraine	dover.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.169.86	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1
184.190.30.34	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
172.98.200.238	147.237.8.46		e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
172.98.200.238	147.237.8.46		e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
223.4.174.30	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
146.185.250.2	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
223.4.174.30	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
223.4.174.30	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.114	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1

01-22-2016-02:04:04 to 01-22-2016-03:04:04

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
37.26.147.186	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
45.51.65.136		147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
109.253.201.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.10.18	Israel	147.237.72.166	aka.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	5
104.187.110.229	United States	147.237.77.176	matpash.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
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
37.26.146.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.161.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
166.171.58.8	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
41.99.55.118	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	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
70.39.185.105	Satellite Provide	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.167.57	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.54.53.65	Israel	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
40.77.167.57	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
137.226.113.7	Germany	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
137.226.113.7	Germany	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
86.1.91.15	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
197.35.110.207	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
37.26.147.186	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
86.1.91.15	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
198.1.101.123	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
119.81.188.158	Hong Kong	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.119	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.29.124.137	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
42.62.74.76	China	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
5.29.124.137	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
218.22.211.69	China	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1

01-22-2016-02:04:04 to 01-22-2016-03:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.250.180.140	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 85.250.180.140	Block	6
41.99.55.118	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.99.55.118	Block	6
41.99.55.118	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1154-ar/	Block	2
109.253.207.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.120.56.7	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
41.230.14.223	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	1
150.70.173.54	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
5.29.2.229	Israel	147.237.77.234	halag.idf.il	Distributed PHP Attempt	Block	1
107.150.45.106	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/size100x0/2413.jpg	Block	1
46.120.56.7	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/xmlrpc.php	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
125.24.80.94	Thailand	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
5.29.2.229	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
68.180.230.167	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1111-he/nakhal.aspx	Block	1
46.120.56.7	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.19.85.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
150.70.173.56	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
5.29.2.229	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 5.29.2.229	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20222-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/1133-22461-he/dover.aspx.	Block	1
46.120.56.7	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
125.24.80.94	Thailand	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
41.130.246.167	Egypt	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
5.29.2.229	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
85.250.180.140	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
46.120.56.7	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.120.56.7	Block	1
46.120.56.7	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
195.154.226.90	France	147.237.72.166	aka.idf.il	Illegal HTTP Version HTTP/	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
40.77.167.1	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/homepage/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	1
46.120.56.7	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
149.88.143.84	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
41.130.246.167	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
5.29.2.229	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1
46.120.98.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.120.56.7	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
197.35.110.207	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
41.99.55.118	Algeria	147.237.77.216	dover.idf.il	Malformed URL www.acunetix.wvs:443	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1398-en/dover.aspx	Block	1
46.120.56.7	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
150.70.173.52	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
41.230.14.223	Tunisia	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
5.29.2.229	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
107.150.45.106	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.219.254.5	Ukraine	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/wp-login.php	Block	1
46.120.56.7	Israel	147.237.76.200	eitan.aka.idf.il	PHP Attempt	Block	1
197.35.110.207	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1

01-22-2016-02:04:04 to 01-22-2016-03:04:04