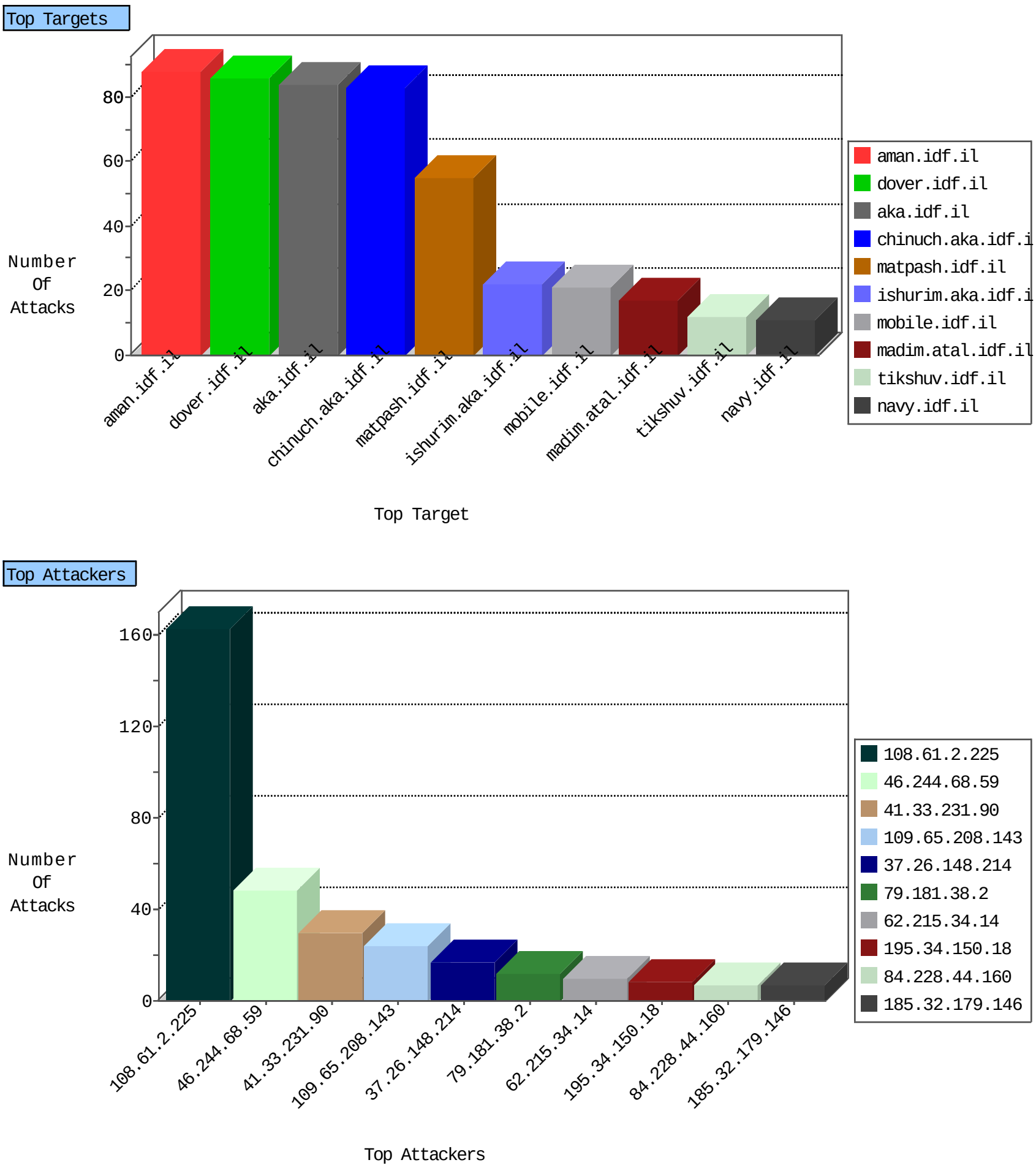
02-12-2016-00:04:06 to 02-12-2016-01:04:06

IDF Under Attack
Daily Report



02-12-2016-00:04:06 to 02-12-2016-01:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.54.237	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
185.130.5.228		147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.179		147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.179		147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

02-12-2016-00:04:06 to 02-12-2016-01:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.215.122	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
88.150.221.26	United Kingdom	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
157.55.39.39	United States	147.237.77.216	dover.idf.il	C158: HTTP(S): Hacked in the Payload	Block	1

02-12-2016-00:04:06 to 02-12-2016-01:04:06

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
62.215.34.14	147.237.72.14	Kuwait	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
62.215.34.14	147.237.8.14	Kuwait	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
212.156.218.109	147.237.76.31	Turkey	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
62.215.34.14	147.237.0.34	Kuwait	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
183.60.252.84	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
51.254.23.230	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN Potential SSH Scan	1
115.236.75.201	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
115.236.75.201	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
80.82.64.68	147.237.0.15	Netherlands	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
62.215.34.14	147.237.76.148	Kuwait	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
62.215.34.14	147.237.8.24	Kuwait	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
62.215.34.14	147.237.0.35	Kuwait	akaws.idf.il	ET SCAN Potential SSH Scan	1
62.215.34.14	147.237.0.33	Kuwait	idf.il	ET SCAN Potential SSH Scan	1
157.55.39.39	147.237.77.216	United States	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	1
51.254.23.230	147.237.8.46	United Kingdom	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
115.236.75.201	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
101.109.146.252	147.237.76.30	Thailand	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.240.192.138	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
62.215.34.14	147.237.76.86	Kuwait	navy.idf.il	ET SCAN Potential SSH Scan	1
62.215.34.14	147.237.8.45	Kuwait	e.eitan.idf.il	ET SCAN Potential SSH Scan	1

02-12-2016-00:04:06 to 02-12-2016-01:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
108.61.2.225	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	79
108.61.2.225	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	77
46.244.68.59	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	47
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
109.65.208.143	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	24
37.26.148.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.181.38.2	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.32.179.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
109.253.216.126	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.76.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.156.157	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.44.160	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.67.121.157	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
109.66.216.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.201		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.61.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.109.212.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.114.167.92	Egypt	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	3
109.67.48.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.33	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.166.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.190.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.16.111.82	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.130.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.7.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.169.237.146	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	2
109.253.132.152	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
108.61.2.225	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	2
157.55.39.66	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
136.243.67.234	Germany	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
66.249.78.239	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
165.215.209.15	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
5.22.130.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.186.96.226	Romania	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	1
5.22.135.205	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.131	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
79.121.224.145	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
46.19.86.172	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
31.210.187.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
84.109.96.253	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.151	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.52.21.124	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

02-12-2016-00:04:06 to 02-12-2016-01:04:06

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
80.82.64.68	Netherlands	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
109.253.210.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
54.163.91.231	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
85.186.96.226	Romania	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

02-12-2016-00:04:06 to 02-12-2016-01:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	6
2.54.158.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.63.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
201.14.93.232	Brazil	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
79.182.197.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.67.57.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.239	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SortDir in eitan.aka.idf.il/938-en/eitan.aspx	None	1
197.166.69.48	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
180.76.15.155	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/templates/shared/usercontrols/headerupper/	Block	1
93.169.119.169	Romania	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
207.46.13.58	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/content.asp	Block	1
86.97.144.89	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
185.120.126.201		147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
109.67.121.157	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
87.69.130.233	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
213.57.153.188	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/selectusertype.asp	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 68.180.228.175	Block	1
198.20.69.74	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
185.120.126.23		147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
93.169.119.169	Romania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
87.69.130.233	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
46.121.232.50	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
185.120.126.201		147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
157.55.39.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	1
87.69.130.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/62312	Block	1
185.120.126.23		147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	1
37.187.201.30	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
93.173.15.58	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion $7 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jeninkilled/stn	Block	1
87.69.130.233	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
46.121.238.73	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 46.121.238.73 (Open Mode)	None	1
193.225.36.84	Hungary	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/idf_in_pictures/hasata/thumb.jpg	Block	1
162.243.38.196	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 162.243.38.196	Block	1
91.148.83.219		147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
201.14.93.232	Brazil	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
185.120.126.201		147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
40.77.167.26	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/miluim/default.aspx	Block	1
95.86.114.29	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ved in www.aka.idf.il/main/rabanut/general.aspx	None	1
87.69.130.233	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
212.199.115.209	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
66.249.64.181	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/589-he/patzar.aspx=	Block	1
197.166.69.48	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
162.243.38.196	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/14-he	Block	1
91.148.83.219		147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
201.14.93.232	Brazil	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
86.97.144.89	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
185.120.126.201		147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1

02-12-2016-00:04:06 to 02-12-2016-01:04:06