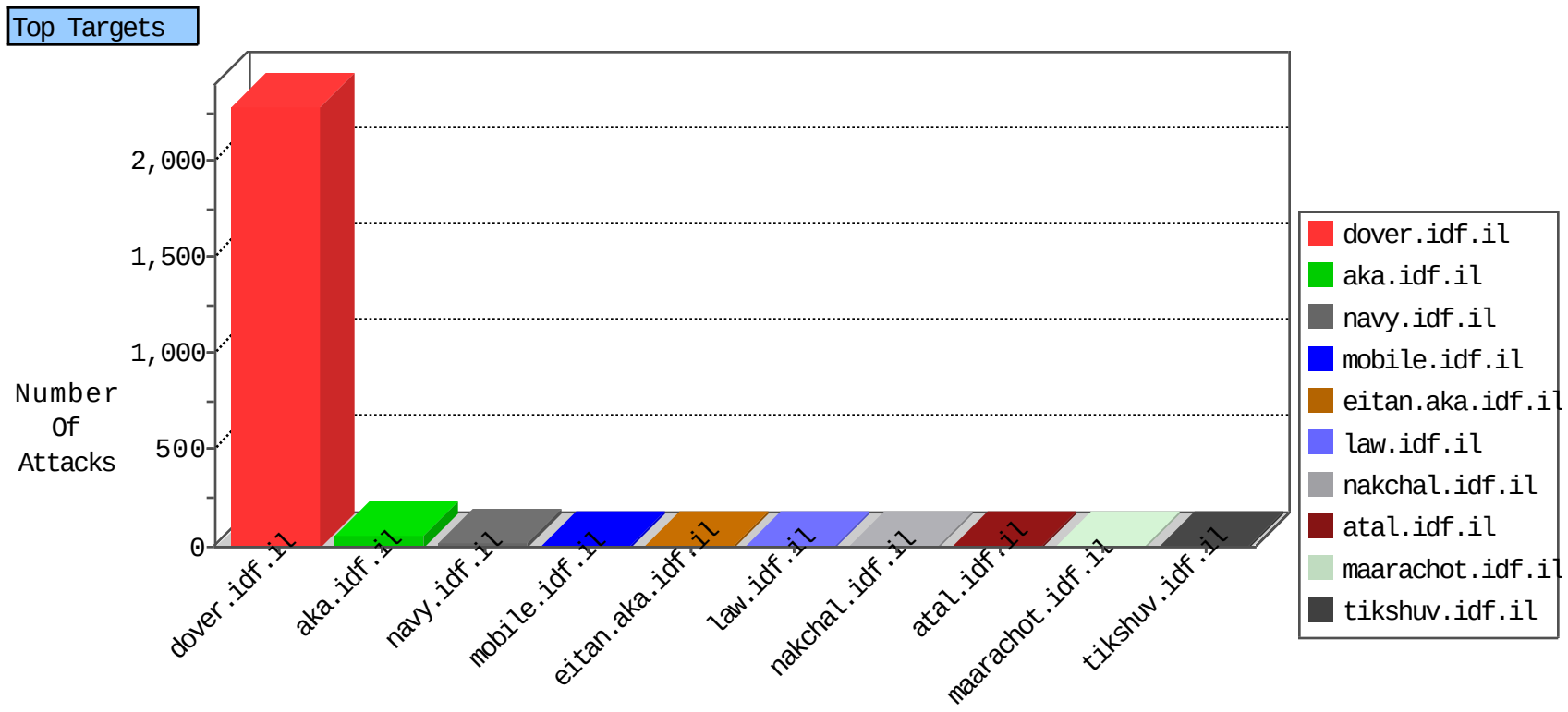
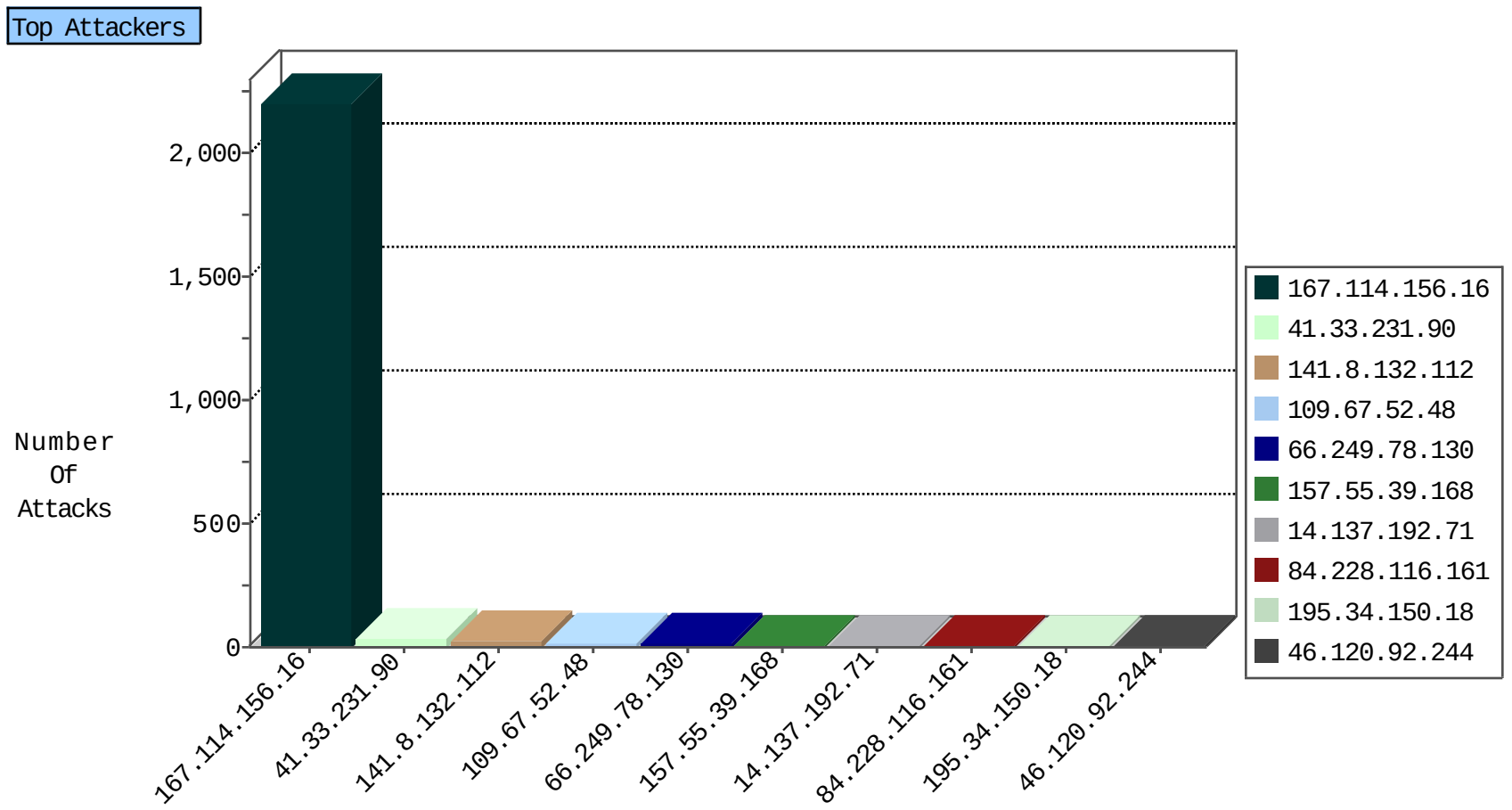
01-23-2016-04:04:05 to 01-23-2016-05:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-23-2016-04:04:05 to 01-23-2016-05:04:05

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	3112
182.143.79.1	China	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
182.143.79.1	China	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
142.54.160.211	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	drop	1
182.143.79.1	China	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
185.40.4.27		147.237.76.200	eitan.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
182.143.79.1	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
182.143.79.1	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
182.143.79.1	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

01-23-2016-04:04:05 to 01-23-2016-05:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.255.162.163	United Kingdom	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
188.165.225.121	France	147.237.76.86	navy.idf.il	0543: HTTP: php.cgi Access	Block	1

01-23-2016-04:04:05 to 01-23-2016-05:04:05

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	3
66.249.66.39	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
163.172.13.173	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sS window 1024	1
159.122.111.166	147.237.76.176	Netherlands	test.ncore.idf.i	ET SCAN NMAP -sS window 1024	1
41.140.253.9	147.237.0.34	Morocco	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
198.20.69.74	147.237.76.34	United States	yohalan.idf.il	ET DROP Dshield Block Listed Source	1
194.187.249.70	147.237.76.30	Europe	himush.idf.il	ET SCAN NMAP -sS window 1024	1
184.173.48.221	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
169.50.77.72	147.237.77.19	Switzerland	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
159.122.111.166	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
159.8.109.19	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
41.140.253.9	147.237.0.34	Morocco	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
218.246.0.97	147.237.76.176	China	test.ncore.idf.i	ET SCAN NMAP -sS window 1024	1
185.40.4.27	147.237.0.19		madim.atal.idf.i	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
172.98.200.237	147.237.77.234		halag.idf.il	ET SCAN NMAP -sS window 3072	1

01-23-2016-04:04:05 to 01-23-2016-05:04:05

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
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
66.249.78.130	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
157.55.39.168	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	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
46.120.92.244	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
14.137.192.71	Australia	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
62.210.209.237	France	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
66.249.64.195	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.120.92.244	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
14.137.192.71	Australia	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	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
66.249.78.160	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
80.108.208.83	Austria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.114	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.20.69.74	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
14.137.192.71	Australia	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
104.130.78.65	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
71.6.165.200	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
184.105.247.244	United States	147.237.0.33	idf.il	drop		drop	1
5.22.135.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
81.169.237.146	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
217.148.45.113	United Kingdom	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
201.202.11.82	Costa Rica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
14.137.192.71	Australia	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
180.252.88.58	Indonesia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
109.10.175.222	France	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.15	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.115.113.84	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
189.79.229.18	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.25.43.94	Germany	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
23.101.61.176	Ireland	147.237.72.166	aka.idf.il	Instant Messengers	instant messenger pattern found, application: Skype	monitor	1
180.252.88.58	Indonesia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
119.81.188.158	Hong Kong	147.237.0.33	idf.il	drop		drop	1
74.82.47.20	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
192.185.4.15	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
159.8.109.19	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
85.25.43.94	Germany	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
208.115.111.73	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
31.168.164.86	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.74	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
119.81.188.158	Hong Kong	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
75.126.221.55	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
216.218.206.104	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.120.92.244	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

01-23-2016-04:04:05 to 01-23-2016-05:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.225.121	France	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 188.165.225.121	Block	3
31.13.113.83	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
173.252.89.56	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
31.13.113.88	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
84.228.116.161	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 84.228.116.161	Block	1
66.249.79.209	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
157.55.39.1	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/contactus/	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/t	Block	1
109.67.52.48	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
104.192.0.18	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.182.96.48	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
109.67.52.48	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
2.52.149.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.52.48	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
84.228.116.161	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.79.239	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
172.245.120.66	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
66.249.64.195	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;catId in www.aka.idf.il/lomdim/pniot/	None	1
109.67.52.48	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	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
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
84.228.116.161	Israel	147.237.76.30	himush.idf.il	Distributed PHP Attempt	Block	1
119.95.128.204	Philippines	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.78.223	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1876	Block	1
109.67.52.48	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 109.67.52.48	Block	1
84.228.116.161	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9169-he/refuah.aspx	Block	1
109.67.52.48	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
66.249.78.2	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.2	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
217.118.64.54	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
84.228.116.161	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/xmlrpc.php	Block	1
119.95.128.204	Philippines	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.254	Block	1
109.67.52.48	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 109.67.52.48	Block	1
84.228.116.161	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
109.67.52.48	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/xmlrpc.php	Block	1
66.249.78.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/general.aspx	Block	1
109.67.52.48	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
217.118.64.54	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
84.228.116.161	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
149.88.110.47	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/general.aspx	Block	1
66.220.156.103	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.52.48	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
84.228.116.161	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
79.182.96.48	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1

01-23-2016-04:04:05 to 01-23-2016-05:04:05