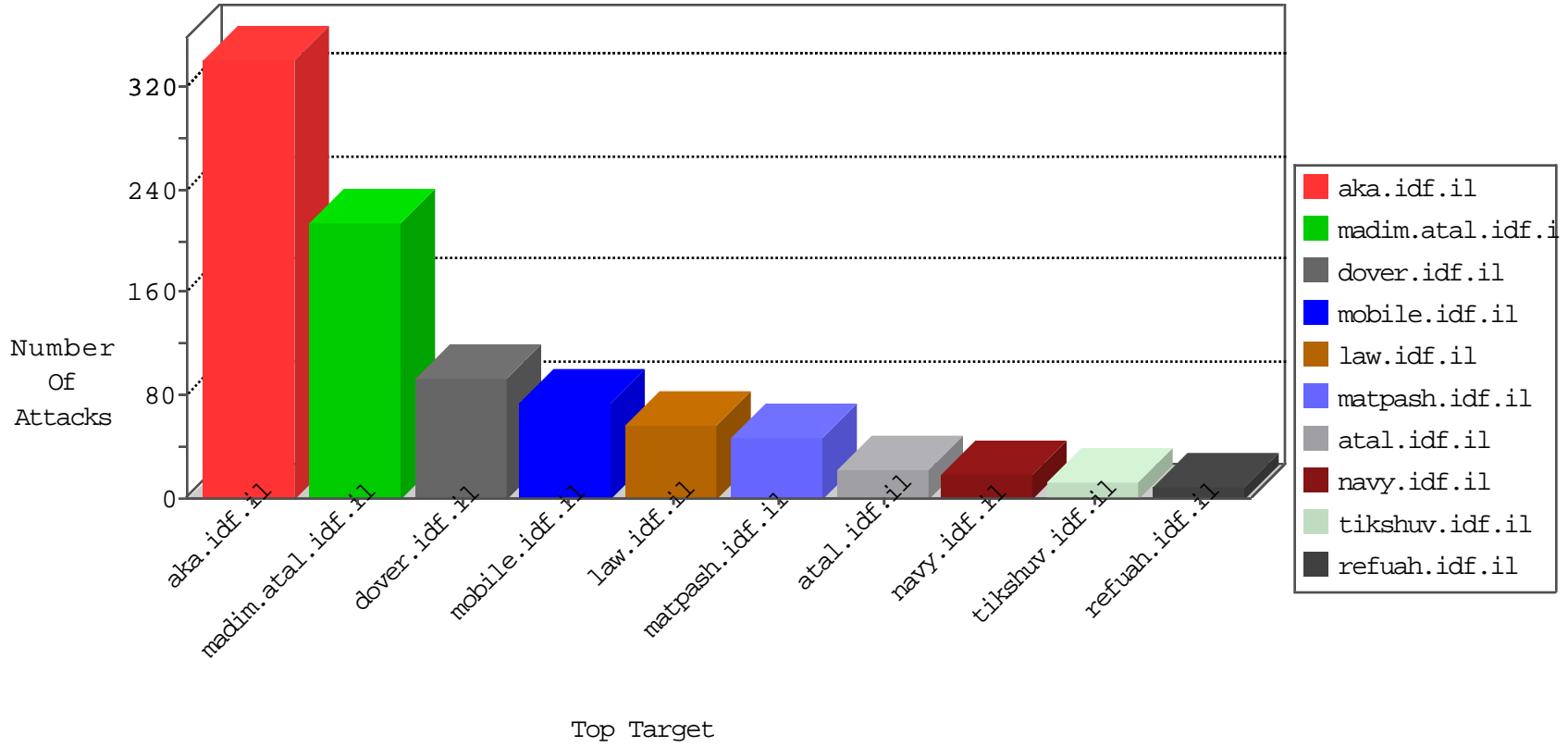


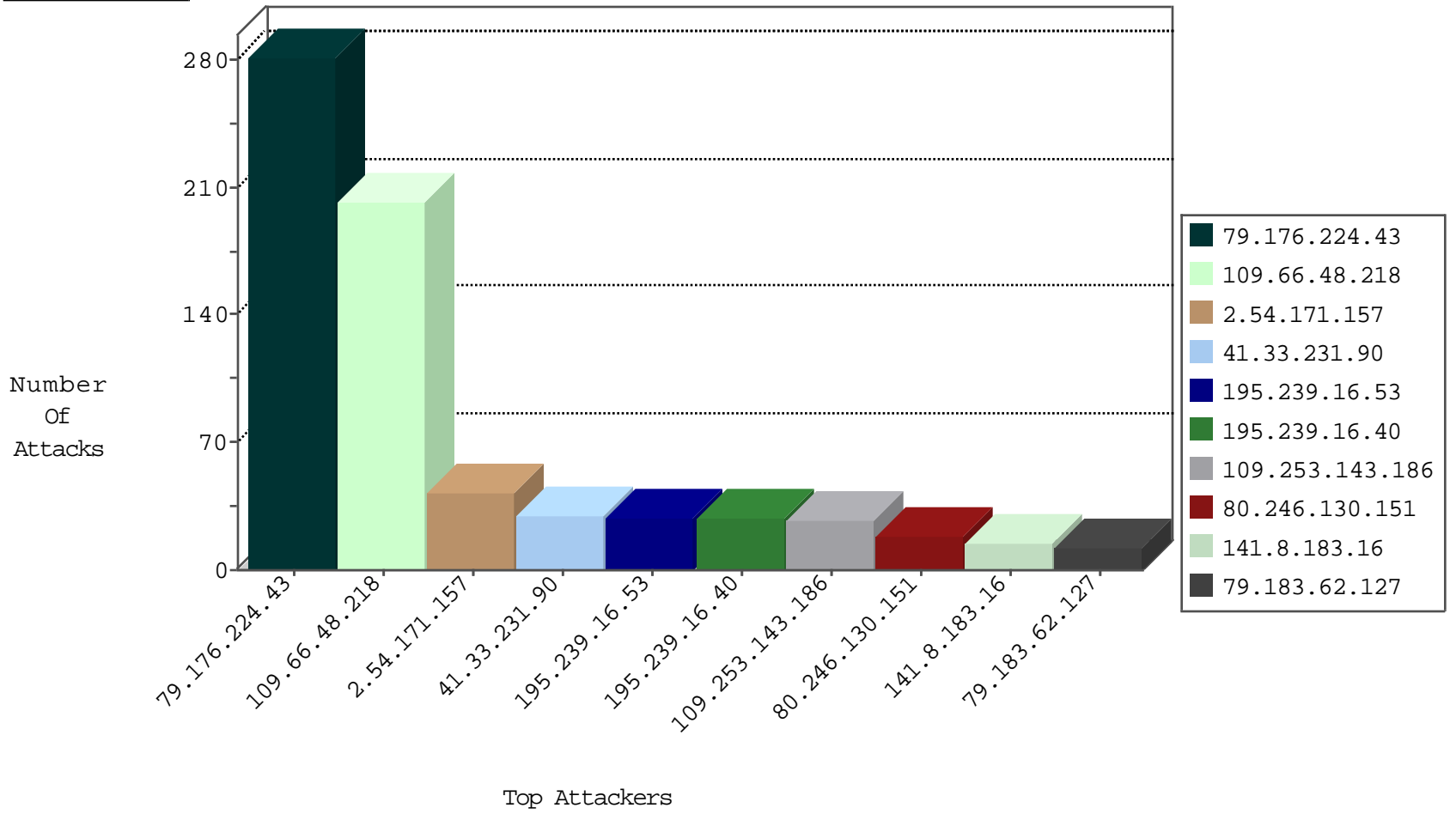
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.174.48.117	Russian Federation	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
120.198.125.244	China	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
120.198.125.244	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
31.186.251.76	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
120.198.125.244	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
155.94.254.143	United States	147.237.72.156	aman.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.151	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.81.212	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
98.119.105.221	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 4096	1
59.45.79.117	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
80.82.64.68	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.103	147.237.76.200		eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
108.59.248.198	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.67	147.237.76.39	Turkey	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.68	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
115.231.9.148	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.176.224.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	282
2.54.171.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
109.253.143.186	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	24
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	24
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
41.227.97.93	Tunisia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	11
5.28.173.68	Israel	147.237.72.166	aka.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	7
80.246.130.151	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
130.193.51.64	Russian Federation	147.237.77.176	matpash.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
94.230.86.251	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.116.43.169	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.255.253.77	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
80.246.130.151	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
130.193.37.23	Russian Federation	147.237.77.176	matpash.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
85.64.202.118	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.65.120.86	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.20.234	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.133.29.225	Ukraine	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
5.102.217.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.64.202.118	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.180.4.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.21.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.146.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.142.68.15	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
108.171.135.165	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.51.45	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.62.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.239.16.53	Russian Federation	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
178.255.215.87	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
130.193.51.98	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
195.239.16.40	Russian Federation	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
178.255.215.87	France	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	2
85.64.125.100	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
185.3.147.121	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.78.170	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
85.64.125.100	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
84.94.174.72	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.168.152.7	United States	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.203	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.243.31.2	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
207.46.13.123	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.178	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.48.218	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.66.48.218	Block	127
109.66.48.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
46.120.177.59	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatquantity.aspx	Block	7
17.138.57.70	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.57.70	Block	6
69.163.208.103	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 69.163.208.103	Block	5
79.183.62.127	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	4
79.183.62.127	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/xmlrpc.php	Block	4
2.54.19.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.171.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_img.asp	Block	2
37.157.219.82	Armenia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
109.65.120.86	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.65.120.86	Block	2
37.157.219.82	Armenia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	2
109.65.120.86	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_imgtop.asp	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	2
85.65.32.11	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
192.99.148.72	Canada	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/phpoadmin/index.php	Block	1
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_pictures.asp	Block	1
66.249.64.108	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
79.183.62.127	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
66.249.78.170	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/1086-en/eitan.aspx	None	1
157.55.39.228	United States	147.237.72.166	aka.idf.il	Unknown Parameter cd5b9038 in www.aka.idf.il/main/home/default.aspx	None	1
95.90.229.218	Germany	147.237.77.216	dover.idf.il	Parameter Type Violation SearchfText in www.idf.il/1065-en/dover.aspx	Block	1
46.254.129.4	Bulgaria	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 46.254.129.4 (Open Mode)	None	1
66.249.78.51	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/2/106462.pdf	Block	1
109.66.48.218	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
66.249.66.60	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/iturim/asp/wars.asp	Block	1
82.0.155.87	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.78.177	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &SortDir in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_imgtop.asp	Block	1
157.55.39.228	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &f in eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
61.102.28.6	Korea, Republic of	147.237.77.74	law.idf.il	PHP Attempt	Block	1
79.183.62.127	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
66.249.78.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/7/112927.pdf	Block	1
130.83.167.219	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.69.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/3044.jpg	Block	1
82.0.155.87	United Kingdom	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.6.59.141	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
61.102.28.6	Korea, Republic of	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
79.183.62.127	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/xmlrpc.php	Block	1
66.249.78.65	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
141.212.122.177	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
45.43.8.118		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
84.229.155.169	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1409-he/atal.aspx	Block	1
69.163.208.103	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_imgtop.asp	Block	1
185.21.121.64	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
66.249.64.48	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/4/105904.pdf	Block	1