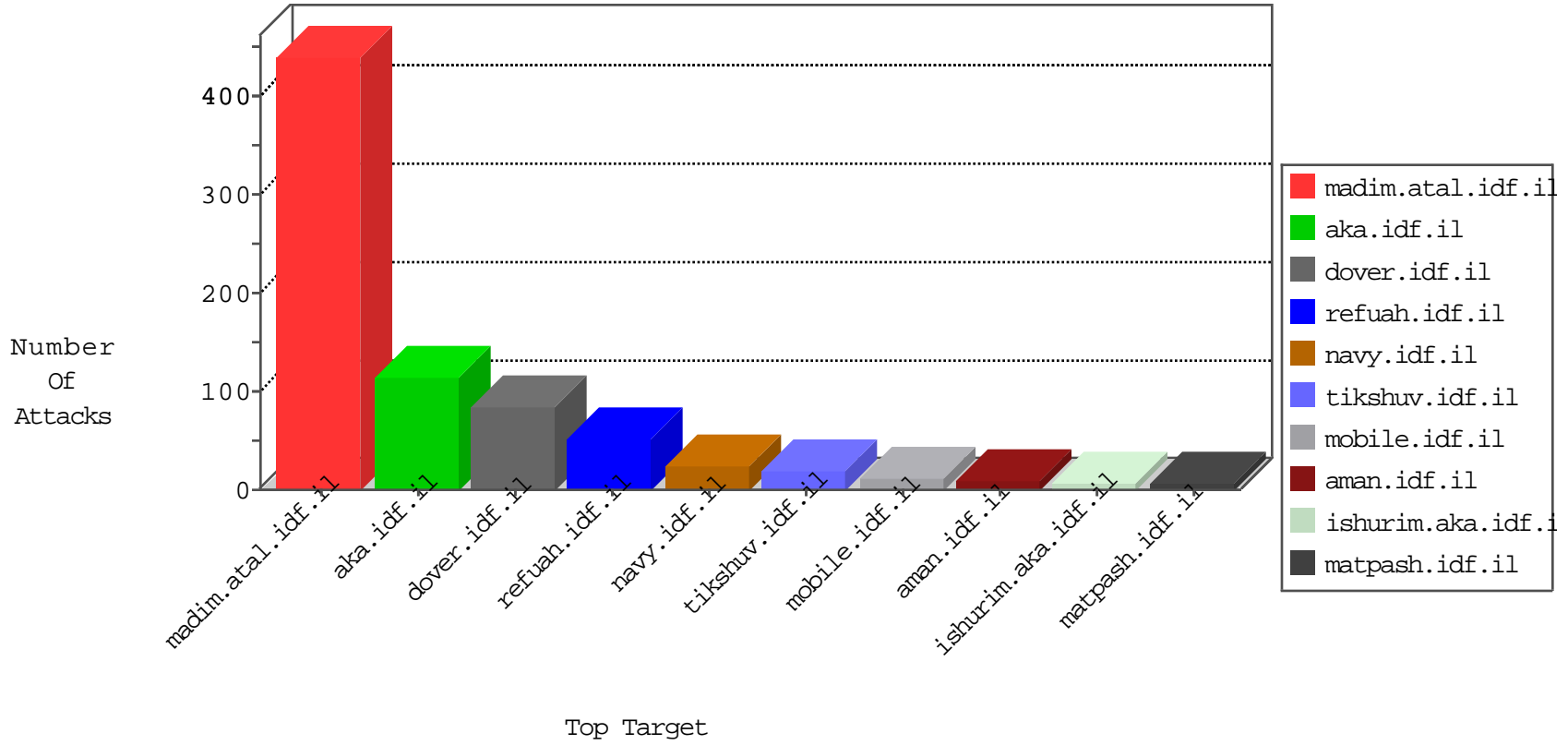


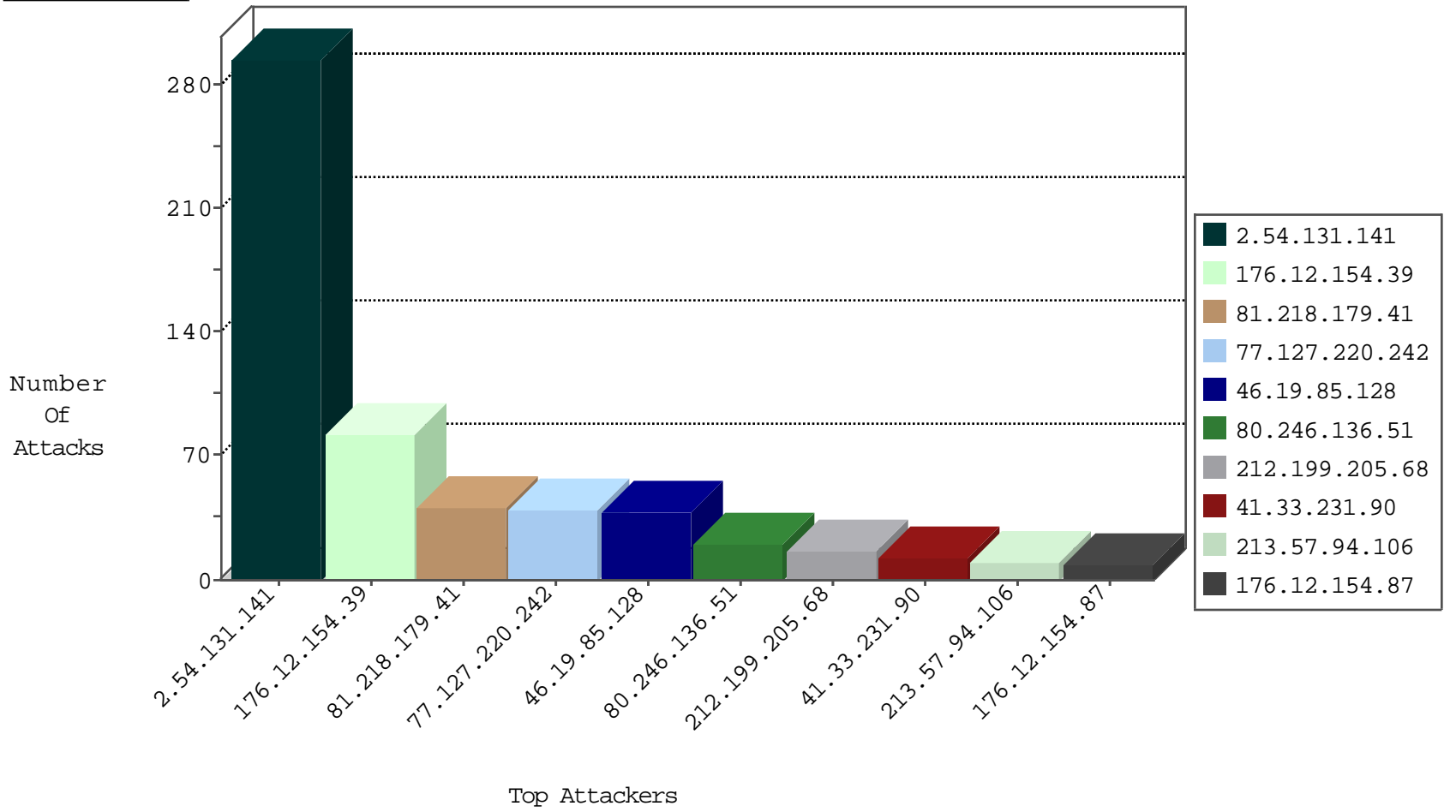
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
204.42.253.2	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.32.210.122	United States	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
88.198.230.79	Germany	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
188.165.15.230	France	147.237.77.234	halag.idf.il	C228: HTTP: AhrefBot crawler	Block	1

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
62.219.120.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
37.200.225.36	147.237.0.200	Oman	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
199.191.56.187	147.237.0.17	United States	m.ny-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
81.218.197.89	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.211	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.191.56.187	147.237.0.17	United States	m.ny-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
146.0.75.114	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
81.218.179.41	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
213.57.94.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.12.154.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
31.168.118.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.12.154.102	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.128.76	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.125.42		147.237.76.86	navy.idf.il	drop	SAM rule	drop	6
217.194.206.108	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
185.3.144.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
24.237.158.10	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
31.210.186.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.111.2.62	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.52.29.26	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.128	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.12.154.61	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.133	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.59.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.138	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.128	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.200.205.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.61.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.12.154.61	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.200.62.41	Ukraine	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
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
40.77.167.34	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
212.25.106.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
5.22.135.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	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
37.26.146.232	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.55	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
141.212.122.184	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.25.106.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
5.29.56.70	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
91.231.193.150	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
74.82.47.12	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.150.97.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
171.25.193.132	Sweden	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
83.244.36.53	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
212.25.106.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.29.133.131	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
137.116.71.170	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.52.21.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.55	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.131.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	150
2.54.131.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	144
176.12.154.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	80
77.127.220.242	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.127.220.242	Block	38
46.19.85.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
80.246.136.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
212.199.205.68	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 212.199.205.68	Block	15
176.12.154.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.65.127.79	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.127.79	Block	3
80.246.136.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.151.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.12.154.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
141.212.122.177	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
41.239.187.186	Egypt	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
83.169.10.185	Germany	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/shared/usercontrols/headerupper/	Block	1
212.5.158.167	Bulgaria	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
46.19.85.176	Israel	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
176.12.154.39	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtStreet in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	1
37.142.226.56	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1523-he/dover.aspx.	Block	1
95.86.102.88	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/&sa=u&ved=0ahukewilhkj599rkahxgwxqkhw x8baqqfggemay&usg=afqjcned8ijyizkxmvasyx7h7flpeujjow	Block	1
217.69.133.68	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/null	Block	1
185.27.219.21	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
66.249.65.246	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
157.55.39.103	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
41.239.187.186	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
84.94.42.42	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder1\$btnAtudaPrint in www.aka.idf.il/main/gyus/atuda/asmachta.aspx	None	1
212.5.158.167	Bulgaria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	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
46.19.85.176	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
37.147.33.61	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation FolderId in www.tikshuv.idf.il/modules/forums/forum.aspx	Block	1
109.67.52.48	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
185.32.179.52	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
66.249.66.64	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/1/111271.pdf	Block	1
157.55.39.168	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
2.54.25.103	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
212.199.205.68	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
46.19.85.176	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method 3e510j45jcfk32zc in URL	Block	1
109.67.52.48	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	1
37.147.33.61	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation ForumId in www.tikshuv.idf.il/modules/forums/forum.aspx	Block	1
81.218.179.41	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
185.32.179.231	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.67	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/3/106183.pdf	Block	1
46.19.85.166	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
85.65.127.79	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
46.210.192.252	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
176.12.155.66	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
141.212.122.177	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
37.147.33.61	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation lang in www.tikshuv.idf.il/modules/forums/forum.aspx	Block	1