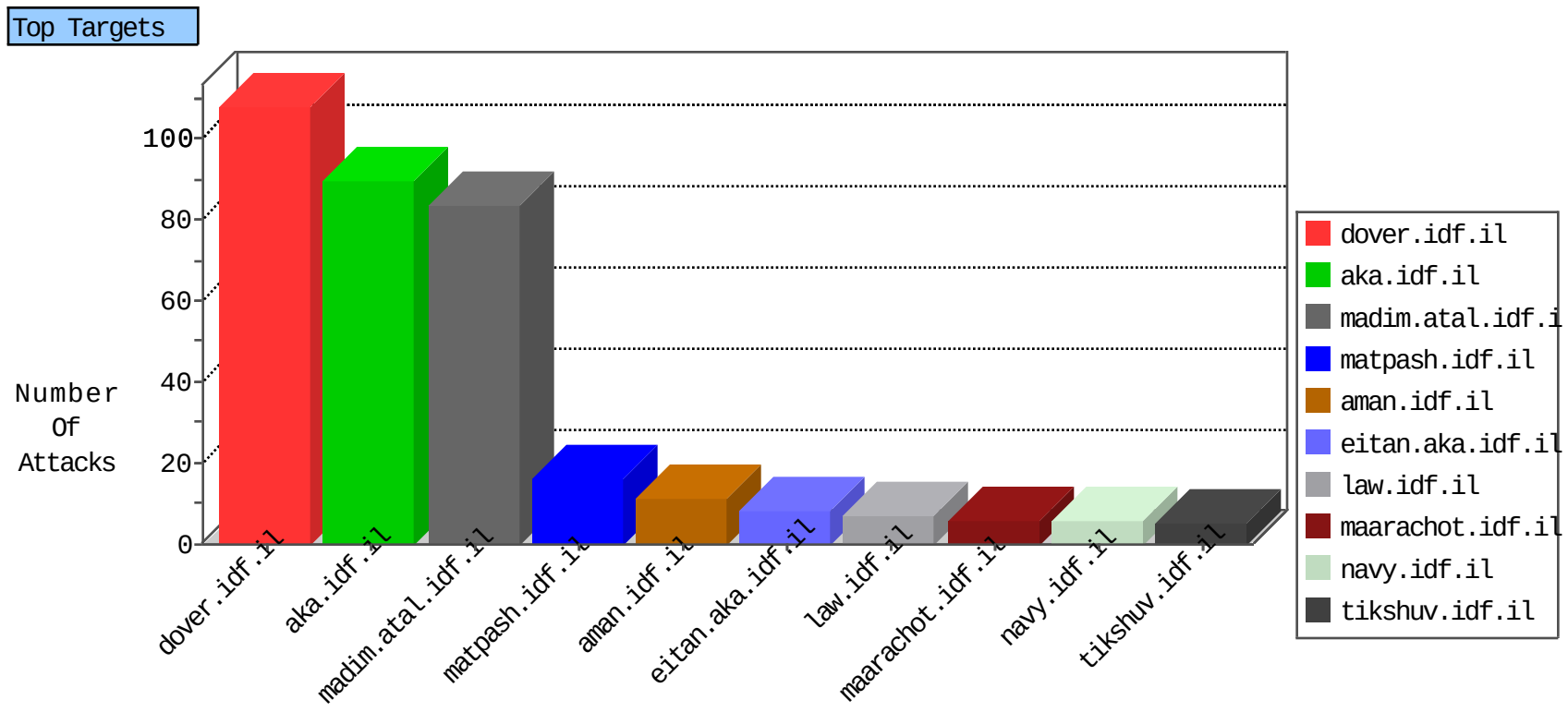
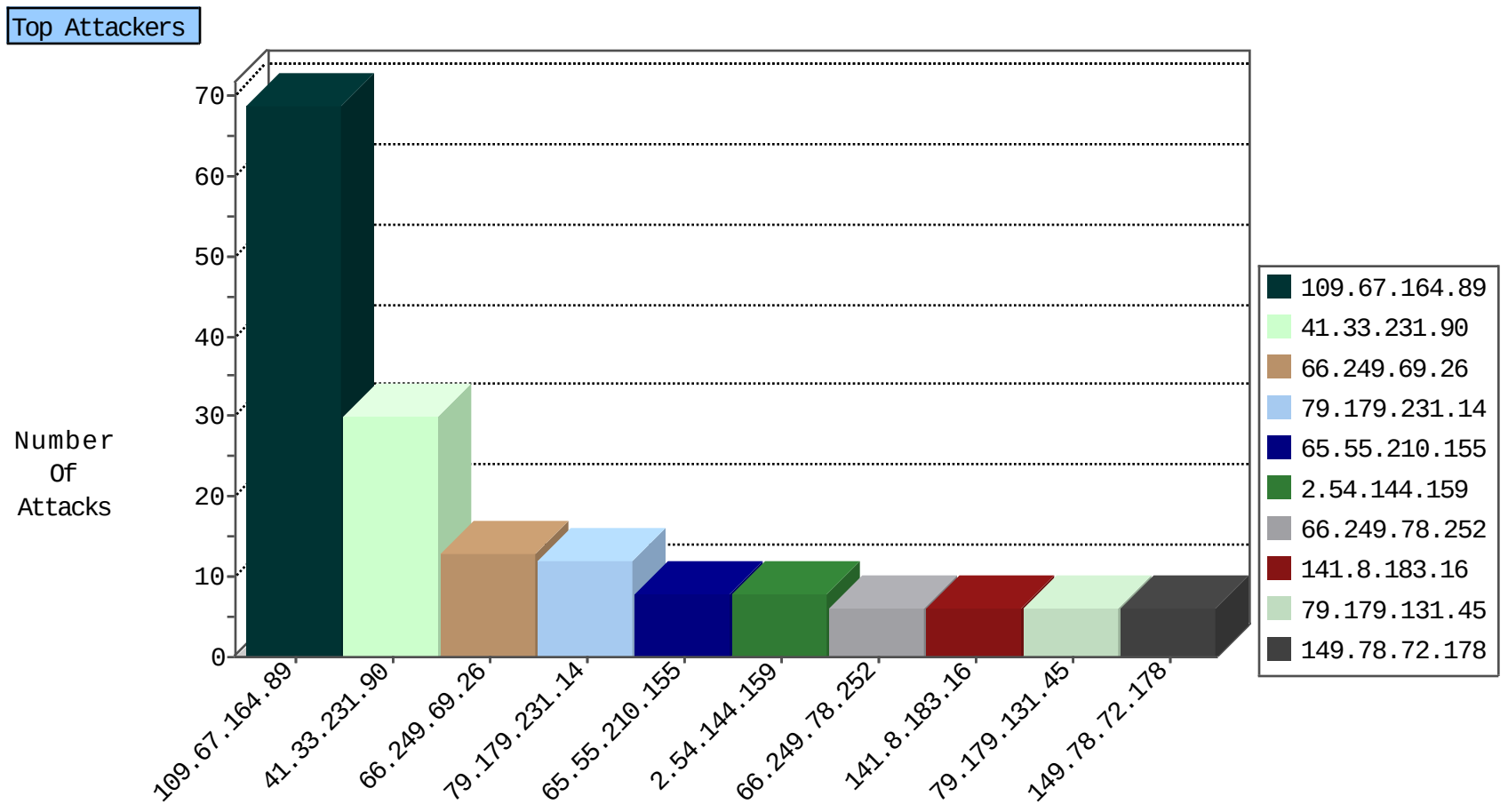
02-13-2016-00:04:06 to 02-13-2016-01:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-13-2016-00:04:06 to 02-13-2016-01:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.130.5.224		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
198.20.99.130	Netherlands	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

02-13-2016-00:04:06 to 02-13-2016-01:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-13-2016-00:04:06 to 02-13-2016-01:04:06

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	3
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.159	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
61.182.170.38	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
46.45.137.67	147.237.77.19	Turkey	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.67	147.237.0.17	Turkey	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.246.0.97	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
112.196.49.101	147.237.72.156	India	aman.idf.il	ET SCAN NMAP -sS window 2048	1
112.196.49.101	147.237.72.156	India	aman.idf.il	ET SCAN NMAP -f -sS	1
61.182.170.38	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
61.182.170.38	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
46.45.137.67	147.237.0.33	Turkey	idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
130.211.100.171	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
112.196.49.101	147.237.72.156	India	aman.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.68	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1

02-13-2016-00:04:06 to 02-13-2016-01:04:06

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	30
79.179.231.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
65.55.210.155	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
66.249.78.252	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.131.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.110.48.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.3.147.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.72.178	Israel	147.237.72.166	aka.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
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
94.230.86.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
130.193.51.64	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	3
150.70.188.171	Japan	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
37.26.147.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.22.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.221.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.23.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.146.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.129.102	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.81.86.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.223	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
77.125.111.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.172	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
93.173.205.97	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
5.22.131.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
130.193.37.23	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
185.37.85.29	Denmark	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
52.49.79.6	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
87.69.235.78	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.86.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
50.18.94.121	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
87.69.235.78	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
84.108.119.196	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.182	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.120.32.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
86.10.103.254	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.205	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.176	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
199.168.142.24	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
46.19.86.174	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.22.131.85	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
178.255.215.87	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
74.91.28.58	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.183	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.120.32.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
86.10.103.254	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

02-13-2016-00:04:06 to 02-13-2016-01:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.164.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	8
2.54.144.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1361-he/dover.aspx	Block	6
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	5
17.138.57.70	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.57.70	Block	4
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.34	Block	3
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.42	Block	2
85.64.86.178	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakhal.idf.il/1120-he/nakhal.aspx	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
46.121.232.50	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
93.109.41.244	Cyprus	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.78.65	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/3/106383.pdf	Block	1
195.174.168.117	Turkey	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
109.67.164.89	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
8.37.70.104	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-he/dover.aspx&usg=alkjrhhwogaqog4zze4wde2ydh8jvxvebg	Block	1
66.249.79.202	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.69.40	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/2389.jpg	Block	1
54.90.107.30	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/â€Ž	Block	1
157.55.39.233	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
2.54.26.57	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 2.54.26.57 (Open Mode)	None	1
93.109.41.244	Cyprus	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
66.249.78.216	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/milluim/index	Block	1
66.249.69.32	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/2934.pdf	Block	1
207.46.13.55	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/home/main/home/default.aspx	Block	1
115.178.26.212	Cambodia	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
8.37.70.140	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-23129-he/dover.aspx&usg=alkjrhjynl80y8u73svylvi_o3ttrdbnng	Block	1
54.159.50.111	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily_statistics/english	Block	1
157.55.39.240	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/shared/usercontrols/navmenu/	Block	1
2.54.26.57	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
105.194.97.140	Egypt	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
212.117.180.21	Luxembourg	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/xmlrpc.php	Block	1
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
115.178.26.212	Cambodia	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
8.37.70.253	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1116-he/dover.aspx&usg=alkjrhjd0wkdbmtpbnboxfnev4i2ae7ndg	Block	1
84.110.33.156	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - 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/4/106394.pdf	Block	1
66.249.64.48	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/3/110763.pdf	Block	1
163.172.7.229	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/documents.asp	Block	1
105.194.97.140	Egypt	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	1
130.83.167.219	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 130.83.167.219	Block	1
66.249.78.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/3/110353.pdf	Block	1
195.174.168.117	Turkey	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
5.175.0.137	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1

02-13-2016-00:04:06 to 02-13-2016-01:04:06