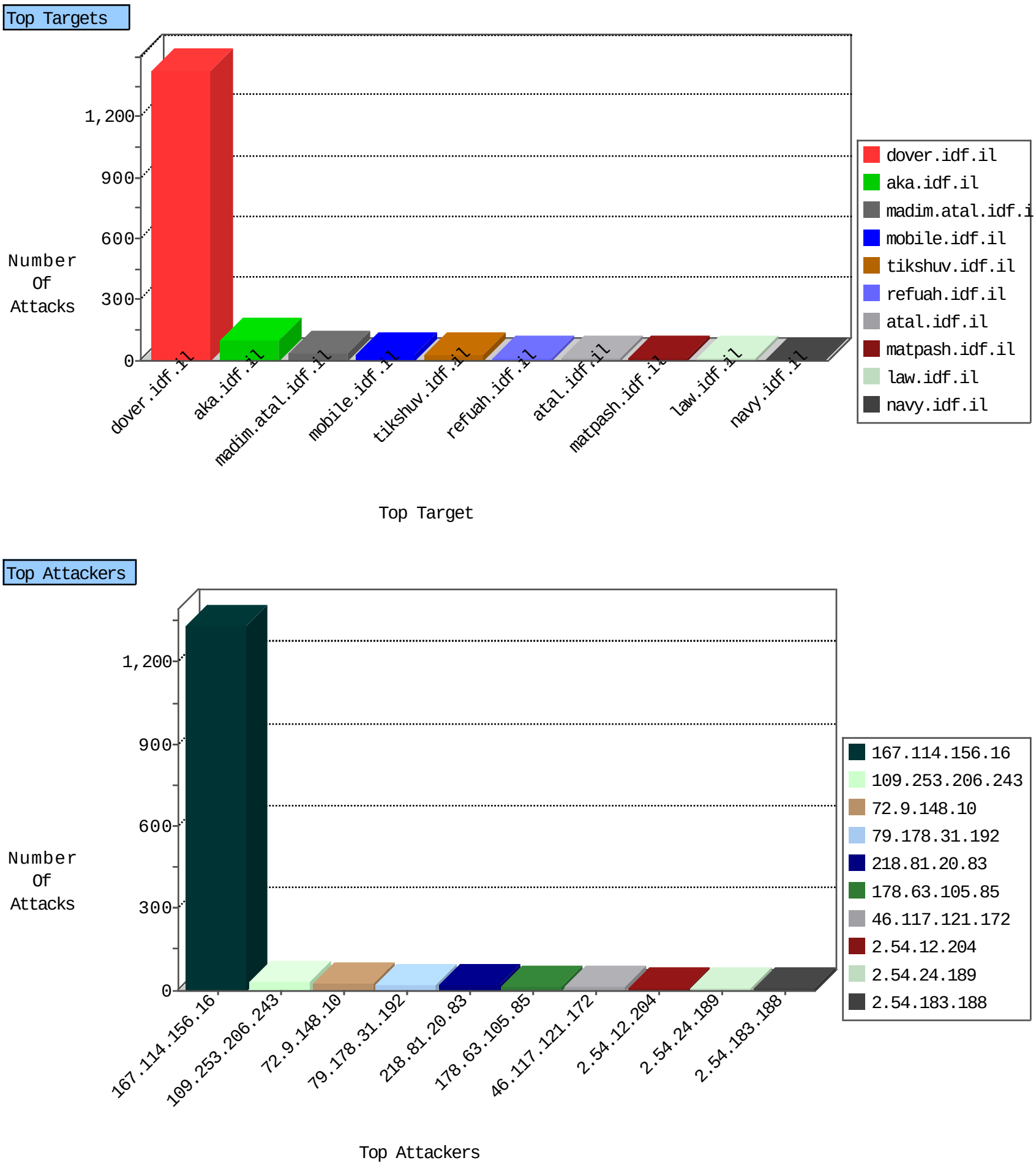
03-13-2016-00:04:06 to 03-13-2016-01:04:06

IDF Under Attack Daily Report



03-13-2016-00:04:06 to 03-13-2016-01:04:06

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	5342
134.147.203.115	Germany	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
51.39.174.239	United Kingdom	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

03-13-2016-00:04:06 to 03-13-2016-01:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.201	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.117	Italy	147.237.72.166	aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

03-13-2016-00:04:06 to 03-13-2016-01:04:06

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	4
218.81.20.83	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
218.81.20.83	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
192.3.9.122	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.81.20.83	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
173.65.154.27	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
119.10.114.32	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 3072	1
218.81.20.83	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
119.10.114.32	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
218.81.20.83	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.81.20.83	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
218.81.20.83	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.114	147.237.76.176	Ukraine	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
218.81.20.83	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.76.44	Sweden	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
89.216.119.94	147.237.76.202		e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
218.81.20.83	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
192.3.9.122	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
218.81.20.83	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
192.3.9.122	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
218.81.20.83	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
178.63.11.208	147.237.8.46	Germany	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
218.81.20.83	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
173.65.154.27	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
218.81.20.83	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
119.10.114.32	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
218.81.20.83	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
119.10.114.32	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
218.81.20.83	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
218.81.20.83	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
89.216.119.94	147.237.76.202		e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
218.81.20.83	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
192.3.9.122	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
89.216.119.94	147.237.76.202		e.halag.idf.il	ET SCAN NMAP -f -sS	1
218.81.20.83	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
192.3.9.122	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1

03-13-2016-00:04:06 to 03-13-2016-01:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
2.54.12.204	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
2.54.183.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.24.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
68.42.125.51	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.69.38	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.211	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.3.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.29.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.75.209.206	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
94.230.86.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.117.121.172	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.i	drop	SAM rule	drop	4
46.117.121.172	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.117.121.172	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.106	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
79.183.168.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
95.86.116.223	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
149.78.236.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.23.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.223.133	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	3
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	3
109.65.56.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.117.121.172	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.183.113.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.116.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.59.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.24.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.174.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.i	drop	SAM rule	drop	3
31.168.192.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.24.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.114.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.11.205	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.141.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.31.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.227.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.160	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
91.200.12.7	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
84.228.215.87	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	2
5.22.135.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

03-13-2016-00:04:06 to 03-13-2016-01:04:06

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	2

03-13-2016-00:04:06 to 03-13-2016-01:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.206.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	35
79.178.31.192	Israel	147.237.0.34	tikshuv.idf.il	Automated Vulnerability Scanning V1	Block	20
176.13.11.205	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	4
5.144.60.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
185.120.126.82		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.11.205	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.13.11.205	Block	2
37.142.64.50	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	1
198.58.103.28	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
157.55.39.193	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
104.185.121.214	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
46.121.154.205	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
207.46.13.192	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
157.55.39.224	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
84.111.165.15	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/site/spotting/spotting.asp	Block	1
31.168.192.251	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
194.2.159.201	France	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/templates/sendtofriend/sendtofriend.aspx parameter f	Block	1
109.67.124.152	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$24 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.64.53	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/7/106667.pdf	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
164.138.116.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
85.64.168.222	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
37.26.148.247	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
194.2.159.201	France	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/templates/sendtofriend/sendtofriend.aspx parameter l	Block	1
66.249.64.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/8/112188.pdf	Block	1
213.57.137.117	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
85.113.97.102	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
37.142.64.50	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xyzzy	Block	1
157.55.39.11	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1137-he/dover	Block	1
66.249.69.38	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
96.240.23.185	United States	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/tizmoret/faq/default.asp	None	1

03-13-2016-00:04:06 to 03-13-2016-01:04:06