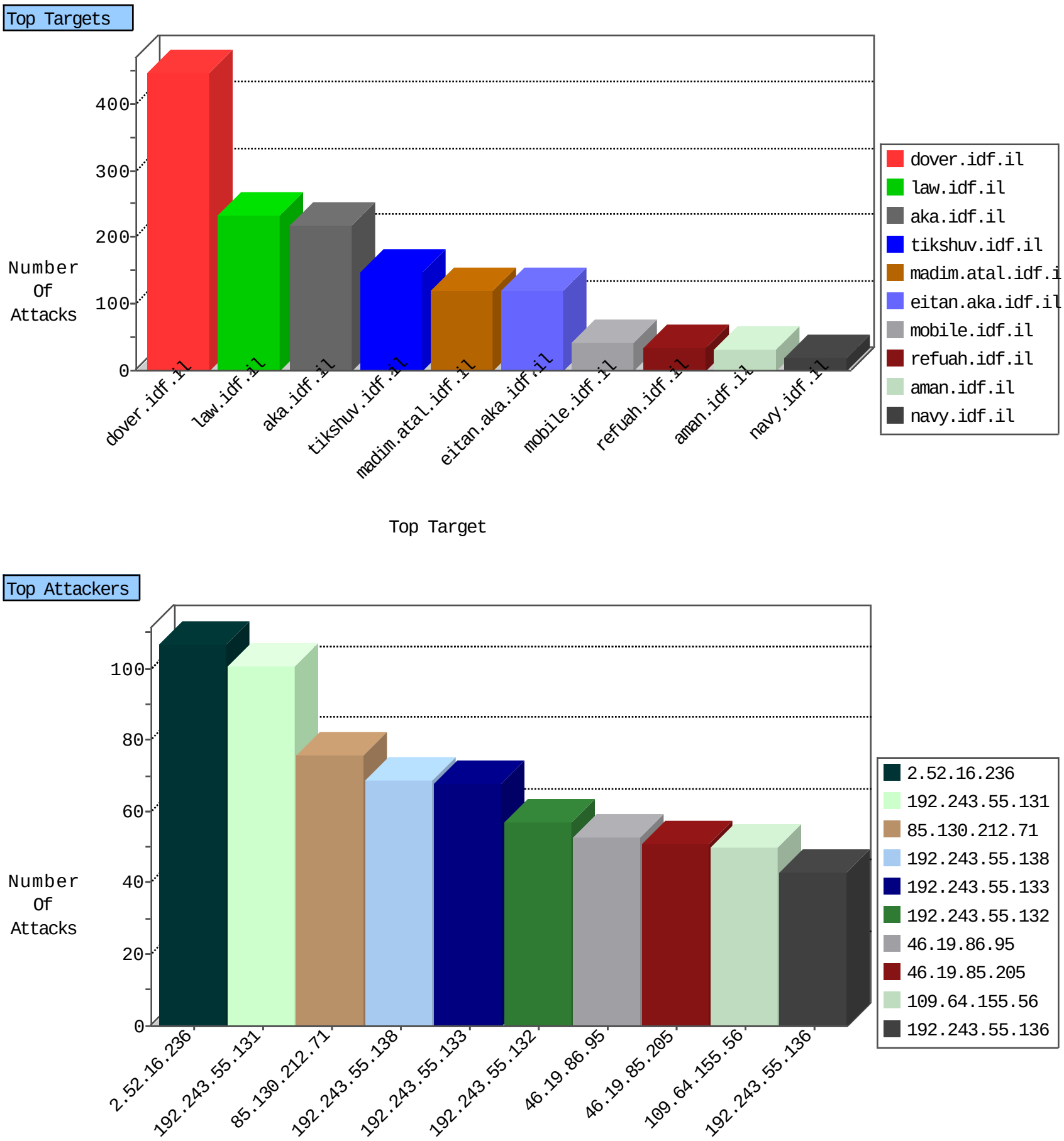
02-20-2016-14:04:02 to 02-20-2016-15:04:02

IDF Under Attack Daily Report



02-20-2016-14:04:02 to 02-20-2016-15:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.130.5.228		147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
112.121.190.9	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
58.114.163.48	Taiwan	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
112.121.190.70	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
58.114.163.48	Taiwan	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
112.121.190.10	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
58.114.163.48	Taiwan	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
112.121.190.71	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
66.249.65.65	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
112.121.190.17	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
58.114.163.48	Taiwan	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.228		147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.138	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
58.114.163.48	Taiwan	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
112.121.190.69	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
58.114.163.48	Taiwan	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

02-20-2016-14:04:02 to 02-20-2016-15:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.108.238.169	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
80.246.133.222	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
176.13.12.82	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
109.65.154.3	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
213.8.204.29	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1

02-20-2016-14:04:02 to 02-20-2016-15:04:02

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
66.249.81.236	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
109.235.254.181	147.237.0.200	Turkey	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
117.10.90.222	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
109.235.254.181	147.237.0.200	Turkey	m4u.idf.il	ET SCAN NMAP -f -sS	1
117.10.90.222	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
117.10.90.222	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
117.10.90.222	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
117.10.90.222	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
117.10.90.222	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
117.10.90.222	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
117.10.90.222	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
117.10.90.222	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
109.235.254.181	147.237.0.200	Turkey	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
117.10.90.222	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
117.10.90.222	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
117.10.90.222	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
117.10.90.222	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
117.10.90.222	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
117.10.90.222	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
117.10.90.222	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1

02-20-2016-14:04:02 to 02-20-2016-15:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.205	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
46.19.86.95	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
85.130.212.71	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	48
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
37.46.39.201	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.85.70	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.54.191.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
85.130.212.71	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
84.110.54.22	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
84.228.5.206	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
79.182.104.102	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
46.116.254.6	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
79.182.104.102	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
80.230.16.24	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
85.130.212.71	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
2.52.16.236	Israel	147.237.0.19	madim.atal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.67.57.211	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.131	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.133	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.182.104.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
79.182.104.102	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
66.249.66.60	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.191.24	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.230.16.24	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.131	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
31.210.187.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.138	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
79.176.28.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

02-20-2016-14:04:02 to 02-20-2016-15:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.16.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
109.64.155.56	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 109.64.155.56	Block	46
2.52.16.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	32
17.138.56.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.56.26	Block	7
2.54.6.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.95	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
46.121.157.119	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
46.19.86.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.66.19.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
203.127.96.234	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.22.81	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1302	Block	2
31.154.172.244	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.109.32.37	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19142-en/dover&hellip	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/patzar	Block	1
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
203.127.96.214	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.159	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
89.120.224.47	Romania	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	1
46.121.136.245	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$2 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.67.57.211	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
79.180.48.116	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
89.120.224.47	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xgf5b3nolwrvy3ncdghpa2fcdhphdmltxdc0ns5kb2m=&infocenteritem=true	Block	1
128.232.110.28	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
79.183.147.246	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$72 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.39	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/	Block	1
184.105.247.196	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
109.64.155.56	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper	Block	1
54.173.223.170	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
128.232.110.28	United Kingdom	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
79.183.191.24	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	1
220.255.148.169	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/documents.asp	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9698-he/refuah.aspx	Block	1
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
199.30.25.81	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.97	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/shared/usercontrols/navmenu/mazi.idf.il	Block	1

02-20-2016-14:04:02 to 02-20-2016-15:04:02