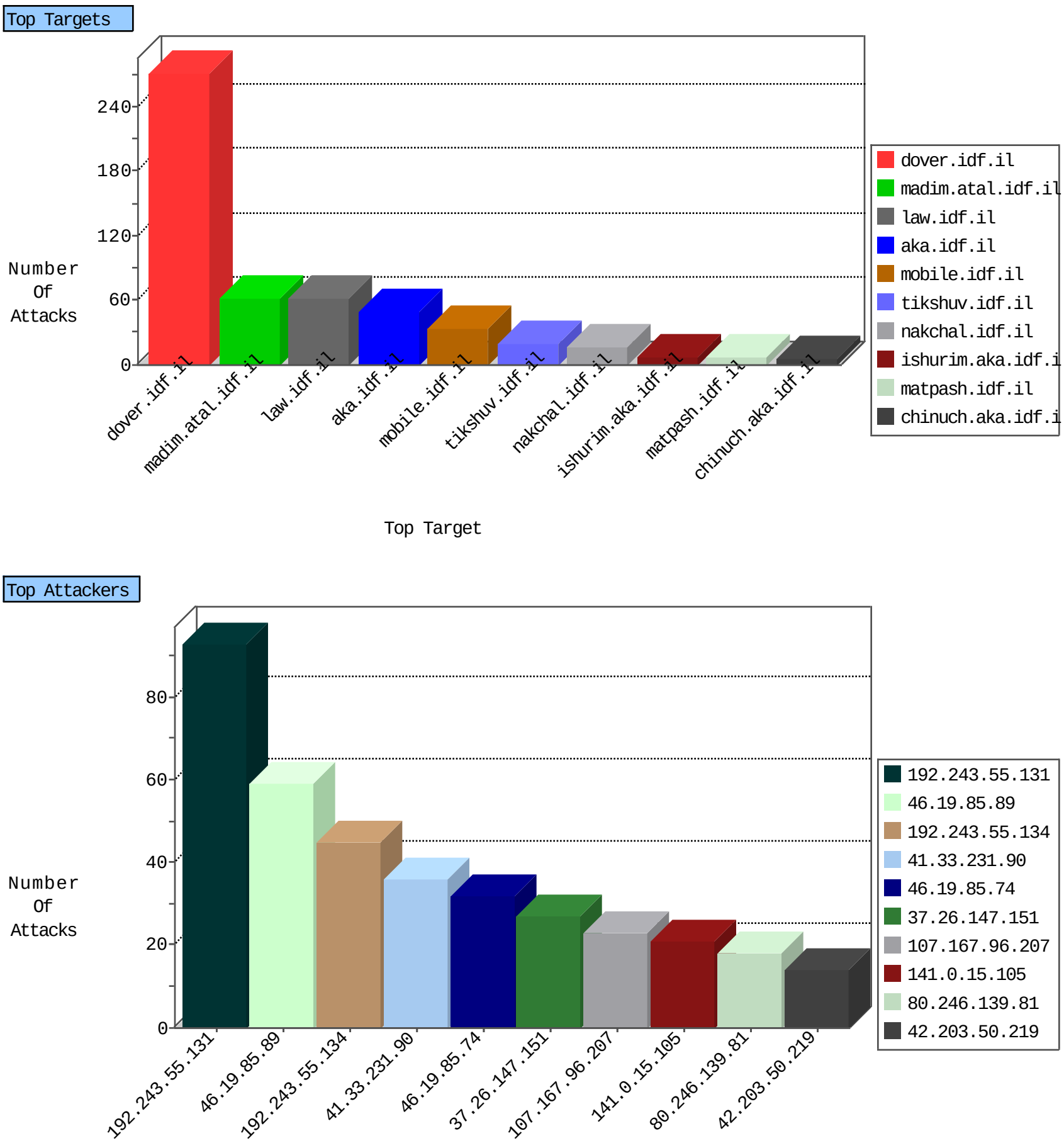
03-04-2016-07:04:03 to 03-04-2016-08:04:03

IDF Under Attack Daily Report



03-04-2016-07:04:03 to 03-04-2016-08:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
1.196.50.110	China	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
216.218.206.91	United States	147.237.77.227	e.hamaz.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.33	Switzerland	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
213.238.176.44	Turkey	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
27.154.48.235	China	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.68	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
213.238.176.44	Turkey	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
81.214.126.75	Turkey	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.88	United States	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
213.238.176.44	Turkey	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
213.238.176.44	Turkey	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1

03-04-2016-07:04:03 to 03-04-2016-08:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.245	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
31.154.154.214	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.117.78.47	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.176.27.53	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.181.234.126	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
93.158.205.89	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	1
109.253.211.231	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-04-2016-07:04:03 to 03-04-2016-08:04:03

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
42.203.50.219	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	2
42.203.50.219	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
42.203.50.219	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
42.203.50.219	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
88.249.106.23	147.237.76.39	Turkey	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
82.118.233.119	147.237.77.176	Bulgaria	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
42.203.50.219	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
42.203.50.219	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
42.203.50.219	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
42.203.50.219	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
42.203.50.219	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
42.203.50.219	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
42.203.50.219	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
82.118.233.119	147.237.77.176	Bulgaria	matpash.idf.il	ET SCAN Potential SSH Scan	1
82.118.233.119	147.237.76.176	Bulgaria	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
42.203.50.219	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
42.203.50.219	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1

03-04-2016-07:04:03 to 03-04-2016-08:04:03

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	36
107.167.96.207	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
141.0.15.105	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
80.246.139.81	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
37.26.147.231	Israel	147.237.77.243	mobile.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	9
192.243.55.131	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.74	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.74	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.147.151	Israel	147.237.77.216	dover.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
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.147.151	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
131.253.25.141	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.147.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.147.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.147.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
37.26.147.151	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
62.219.194.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.123.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.22.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.164.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.176.62.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.65.82.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.110.7.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.151.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.67.235.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.64.14.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.183.66.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-04-2016-07:04:03 to 03-04-2016-08:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	4
176.13.20.174	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1302	Block	3
87.68.240.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.20.174	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.13.20.174	Block	3
208.80.155.217	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.80.155.217	Block	1
66.249.66.182	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/9/729.pdf	Block	1
2.54.2.21	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
188.165.208.29	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
112.215.63.11	Indonesia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
208.80.155.217	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
178.255.215.87	France	147.237.76.147	chinuch.aka.idf.i	Unknown Parameter l in www.chinuch.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
79.181.123.67	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
37.237.128.110	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19142-en/dover&hellip	Block	1
113.88.27.151	China	147.237.77.216	dover.idf.il	Multiple URL is Above Root Directory from 113.88.27.151	Block	1
66.249.66.64	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/6/110326.pdf	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20386-he/kkkkkkk=c44bc6dakkkkkkk_c44bc6da	Block	1
79.182.115.156	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
40.77.167.20	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-23092-he/dover.aspx	Block	1
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	1
131.253.25.146	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.66.126	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/5/108455.pdf	Block	1
185.99.32.3		147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 185.99.32.3 (Open Mode)	None	1
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
66.249.66.179	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/6/1096.pdf	Block	1
2.54.2.21	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
185.112.248.32		147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
109.253.156.221	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.102.9.81	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1

03-04-2016-07:04:03 to 03-04-2016-08:04:03