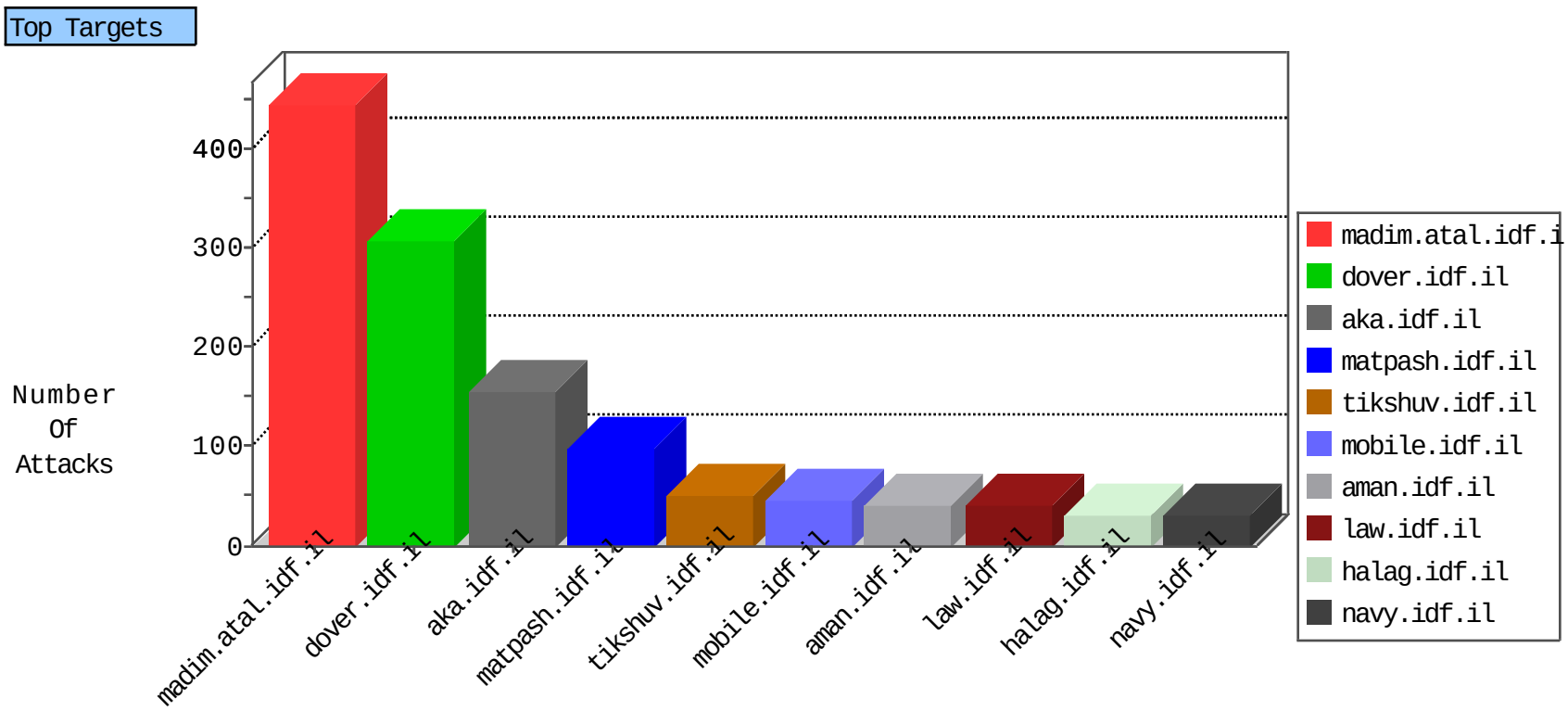
03-04-2016-16:04:07 to 03-04-2016-17:04:07

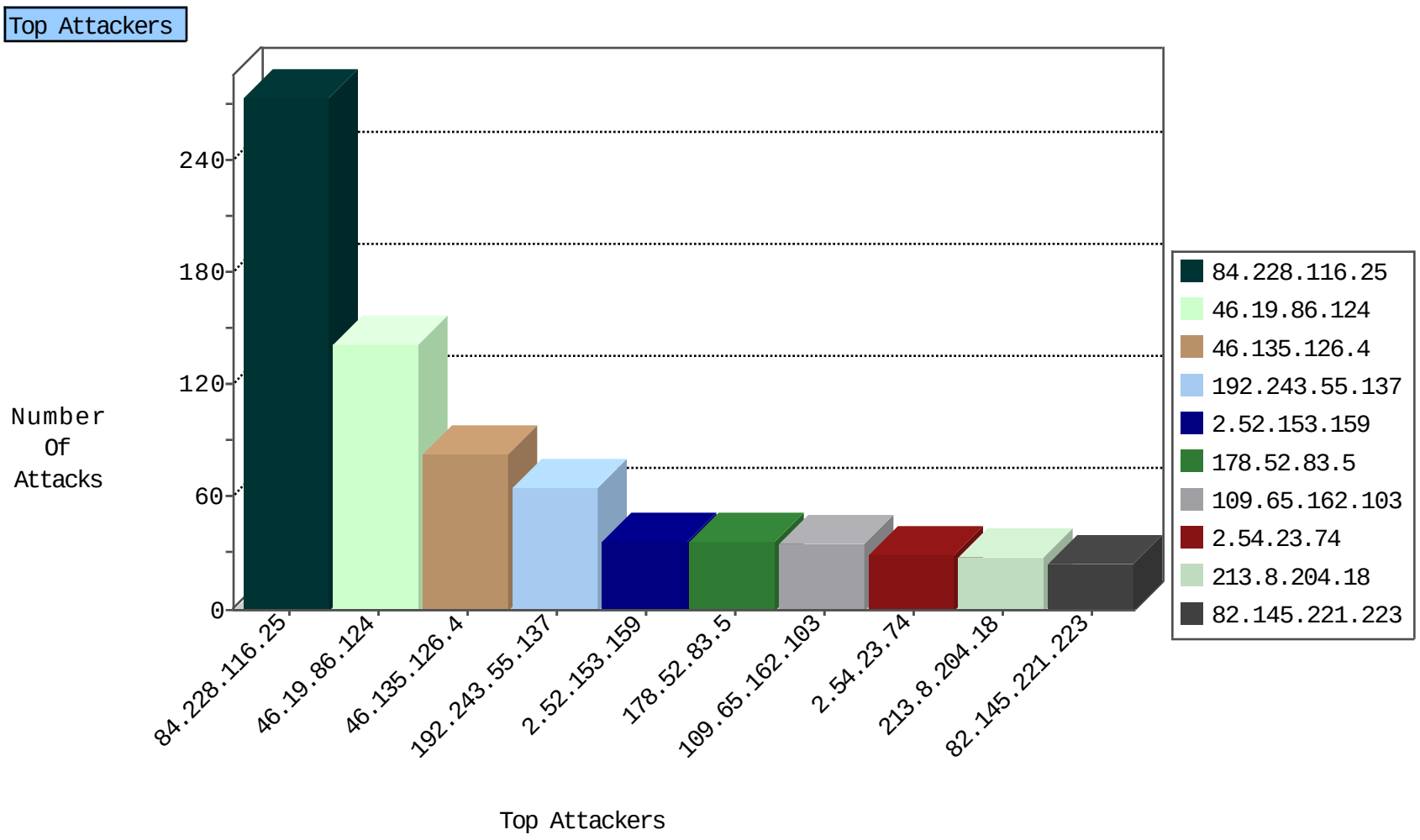
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

03-04-2016-16:04:07 to 03-04-2016-17:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.221.223	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	25
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
82.145.216.53	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
82.145.221.135	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
179.43.144.33	Switzerland	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
207.104.161.245	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

03-04-2016-16:04:07 to 03-04-2016-17:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.22.135.139	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
66.249.93.101	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
66.249.93.97	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
66.249.93.105	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
46.121.200.201	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.177.115.236	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.253.218.210	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.93.97	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
207.46.13.96	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	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
66.249.93.101	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-04-2016-16:04:07 to 03-04-2016-17:04:07

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
185.72.179.221	147.237.77.226		www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.221	147.237.77.205		prisha.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.221	147.237.77.170		maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
23.125.172.41	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
208.116.37.210	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
186.116.16.161	147.237.76.30	Colombia	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.72.179.221	147.237.77.233		atal.idf.il	ET SCAN NMAP -sS window 1024	1
185.72.179.221	147.237.77.216		dover.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.221	147.237.77.179		e.mazi.idf.il	ET SCAN Potential SSH Scan	1
23.125.172.41	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
23.125.172.41	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
209.126.116.147	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
185.72.179.221	147.237.77.235		sviva.idf.il	ET SCAN Potential SSH Scan	1

03-04-2016-16:04:07 to 03-04-2016-17:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.135.126.4	Czech Republic	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	67
109.65.162.103	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
2.54.23.74	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
178.52.83.5	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
178.52.83.5	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
46.135.126.4	Czech Republic	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
2.52.153.159	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
213.8.204.18	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	14
213.8.204.18	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
5.122.18.223	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
109.65.162.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.85.243	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.182.189.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.182.152.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
31.168.200.149	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.153.159	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.228.213.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.135.139	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.122.18.223	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.177.135.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.157.64	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
109.65.69.91	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.64.68.18	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.137	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.180.15.123	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.180.15.123	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	4
109.64.198.238	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.253.218.210	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.110.211.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.23.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.102.254.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.62.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.153.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
37.26.146.245	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.181.60.226	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	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

03-04-2016-16:04:07 to 03-04-2016-17:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.228.116.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	274
46.19.86.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	142
46.19.86.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
213.57.208.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
2.54.23.74	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
201.6.147.203	Brazil	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
109.186.49.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.30.24.216	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
87.69.105.241	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
109.253.141.37	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.253.141.37	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
149.255.196.51	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
85.64.126.18	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
66.249.69.81	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1399-he/atal.aspx	Block	1
109.65.162.103	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
85.64.126.18	Israel	147.237.77.216	dover.idf.il	Multiple NULL Character in Header Name from 85.64.126.18	Block	1
85.64.126.18	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
5.29.162.166	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Distributed Unknown HTTP Request Method	Block	1
84.108.240.97	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
136.243.67.234	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
85.64.126.18	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
65.242.178.130	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.148.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.64.126.18	Israel	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Header Value from 85.64.126.18	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Method	Block	1
85.64.126.18	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name NàIîœg§,}&,ôeýŸ–	Block	1
66.249.69.97	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/926-he/atal.aspx	Block	1
109.65.194.185	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
46.19.86.140	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
85.64.126.18	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 85.64.126.18	Block	1
85.64.126.18	Israel	147.237.77.216	dover.idf.il	Malformed HTTP Header Line 7	Block	1
31.13.130.178	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation &l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
181.170.15.157	Argentina	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
136.243.105.99	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
84.111.108.23	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
85.64.126.18	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method ×ý[<[[#14]]«å[[#25]][[#22]]ãeŸ•ÿ†[[#0]]¬íÏ#[[#15]])Ð¹[[#6]]`Ôþ¯z	Block	1
66.249.64.243	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/news/news.in.aspx	Block	1
37.77.49.239	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
201.6.147.204	Brazil	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.64.126.18	Israel	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 85.64.126.18	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Distributed Abnormally Long Request	Block	1
85.64.126.18	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Value	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1384-he/dover.aspx	Block	1
85.64.126.18	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 85.64.126.18 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
60.52.84.212	Malaysia	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
85.64.126.18	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
31.168.200.149	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
195.154.173.103	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
138.36.0.3		147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/index.php	Block	1

03-04-2016-16:04:07 to 03-04-2016-17:04:07