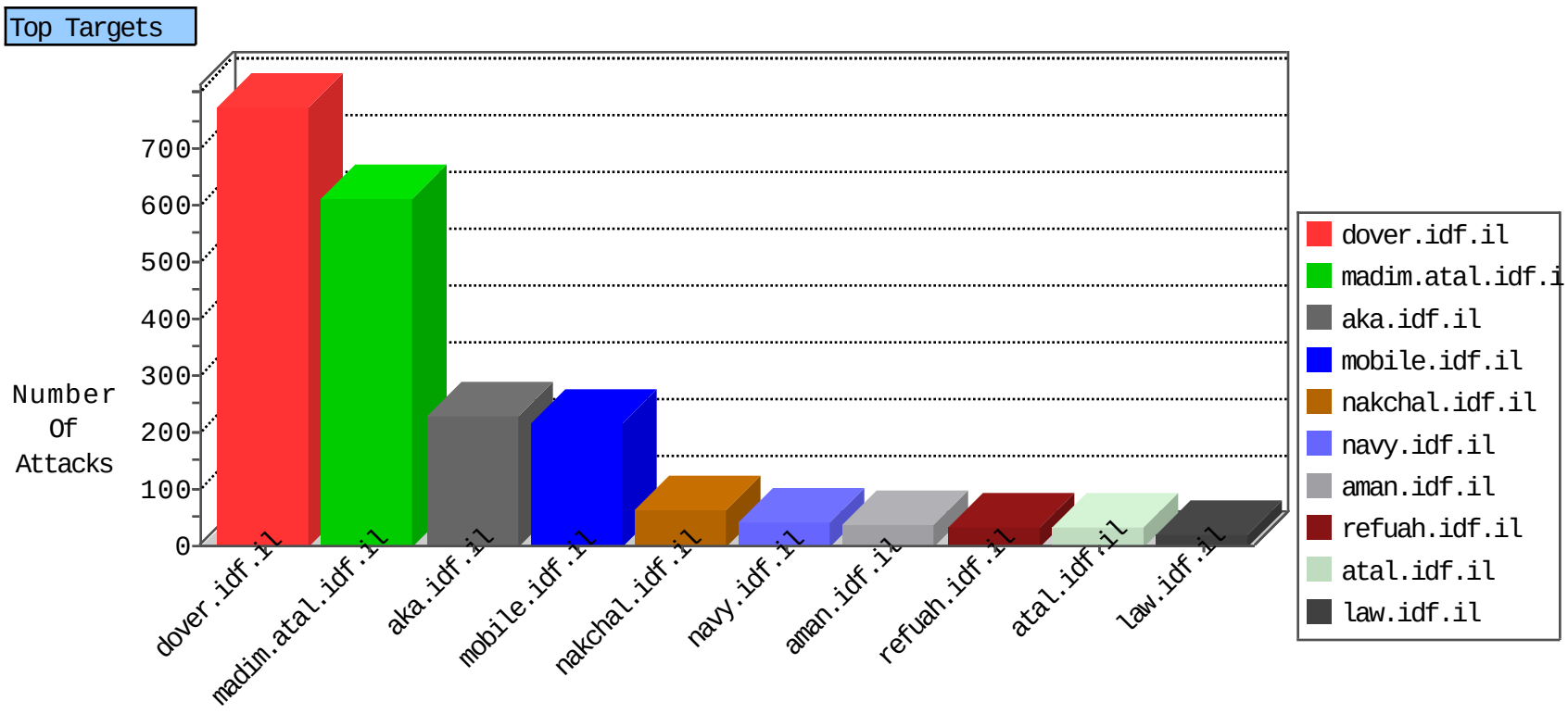
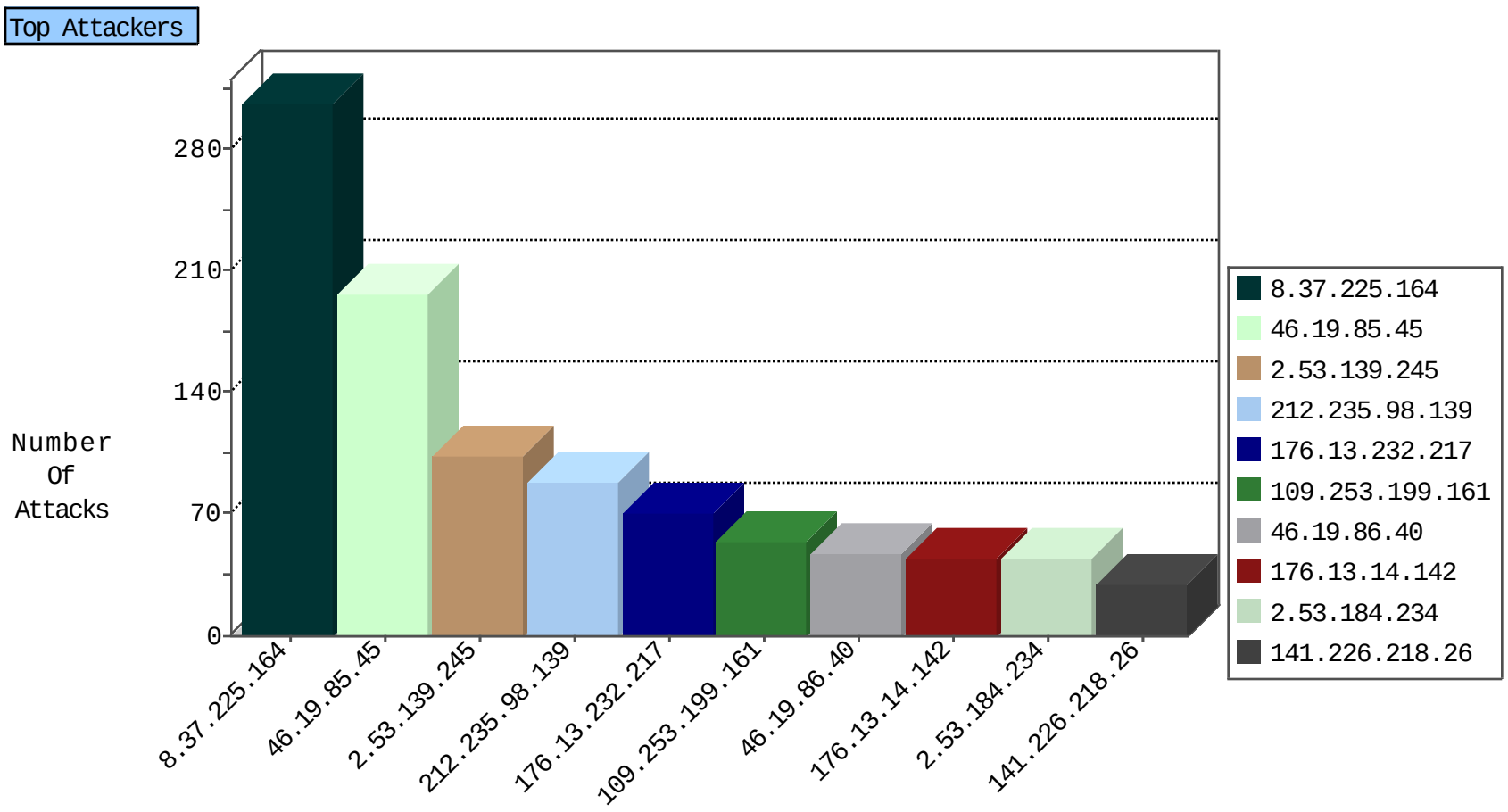
10-05-2016-14:04:04 to 10-05-2016-15:04:04

IDF Under Attack
Daily Report

Top Targets



Top Attackers



10-05-2016-14:04:04 to 10-05-2016-15:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.247.237	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	9
62.219.194.190	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
176.13.2.41	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
109.253.133.210	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
194.90.217.88	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	4
62.0.225.254	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	4
8.37.225.164	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
68.180.229.178	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
81.218.251.251	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
93.174.94.235	Netherlands	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
109.67.63.93	Israel	147.237.72.166	aka.idf.il	Black List	drop	1
109.253.133.210	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1

10-05-2016-14:04:04 to 10-05-2016-15:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.130	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
173.234.159.250	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
2.55.55.224	Israel	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
106.120.188.147	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

10-05-2016-14:04:04 to 10-05-2016-15:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
45.56.125.54	147.237.76.199	United States	e.nakchal.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
213.57.195.191	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
54.144.74.221	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
194.54.168.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.161.40.17	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
188.120.148.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.161.40.17	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.27.106.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
114.112.83.142	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
14.152.59.11	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
109.65.70.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
83.130.68.52	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.101.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
54.144.74.221	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
213.57.127.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.229.223.8	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
192.114.3.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.161.40.17	147.237.0.33	Russian Federation	idf.il	ET SCAN NMAP -sS window 1024	1
185.56.82.22	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.86.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.72.135.147	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.21.80	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.206.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
14.152.59.11	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
90.254.151.79	147.237.0.34	United Kingdom	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.178.198.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.138.2.30	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1

10-05-2016-14:04:04 to 10-05-2016-15:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.225.164	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	304
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
2.53.184.234	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
141.226.218.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
109.253.193.159	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.85.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
141.226.162.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
79.177.121.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.121.64.243	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
46.19.86.249	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
62.0.225.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.116.36.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
196.53.45.108	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	12
199.203.215.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.55.166.35	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
78.32.113.34	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
212.235.98.139	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.189	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
46.32.205.6	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	11
46.32.205.6	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
62.0.222.1	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	10
141.226.162.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.144	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	10
109.253.133.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.51	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
141.226.161.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
196.53.45.108	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
109.253.222.37	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.42	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
141.226.162.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
62.0.197.69	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.85	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
82.81.90.118	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.55.135.18	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.50.132.39	United Arab Emirates	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
93.172.110.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
93.172.110.61	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
80.246.139.200	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
176.13.15.225	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.226.162.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.154.81.78	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.139.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
100.92.143.25		147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	5
31.168.166.86	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.60	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

10-05-2016-14:04:04 to 10-05-2016-15:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	197
2.53.139.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
176.13.232.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
109.253.199.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
46.19.86.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
176.13.14.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
176.13.10.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
80.246.139.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.19.85.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
80.246.136.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
109.253.200.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
82.166.24.134	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	8
46.19.85.48	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
81.218.70.243	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 81.218.70.243	Block	6
109.253.222.37	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
109.253.193.159	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
176.13.242.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
82.166.24.134	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 82.166.24.134	Block	5
62.219.174.67	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	4
82.166.24.134	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/4/	Block	3
62.219.174.67	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 62.219.174.67	Block	3
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.8.71.26	Block	3
82.80.30.139	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
79.177.121.208	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
213.151.55.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/glyus	Block	2
82.166.97.26	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	2
2.53.150.179	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.177.144.175	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
77.138.237.4	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	2
2.55.166.35	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.58	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	2
77.127.7.16	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
46.120.23.14	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	1
212.199.121.196	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/rules.abe	Block	1
81.218.70.243	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/0/470.jpg	Block	1
176.13.229.227	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
77.139.21.47	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
5.102.242.206	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Malformed URL	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/sitemap.aspx	Block	1
185.32.176.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.101	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
37.26.149.255	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.26.149.255	Block	1
77.127.15.248	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.147.122	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
148.251.179.145	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1

10-05-2016-14:04:04 to 10-05-2016-15:04:04