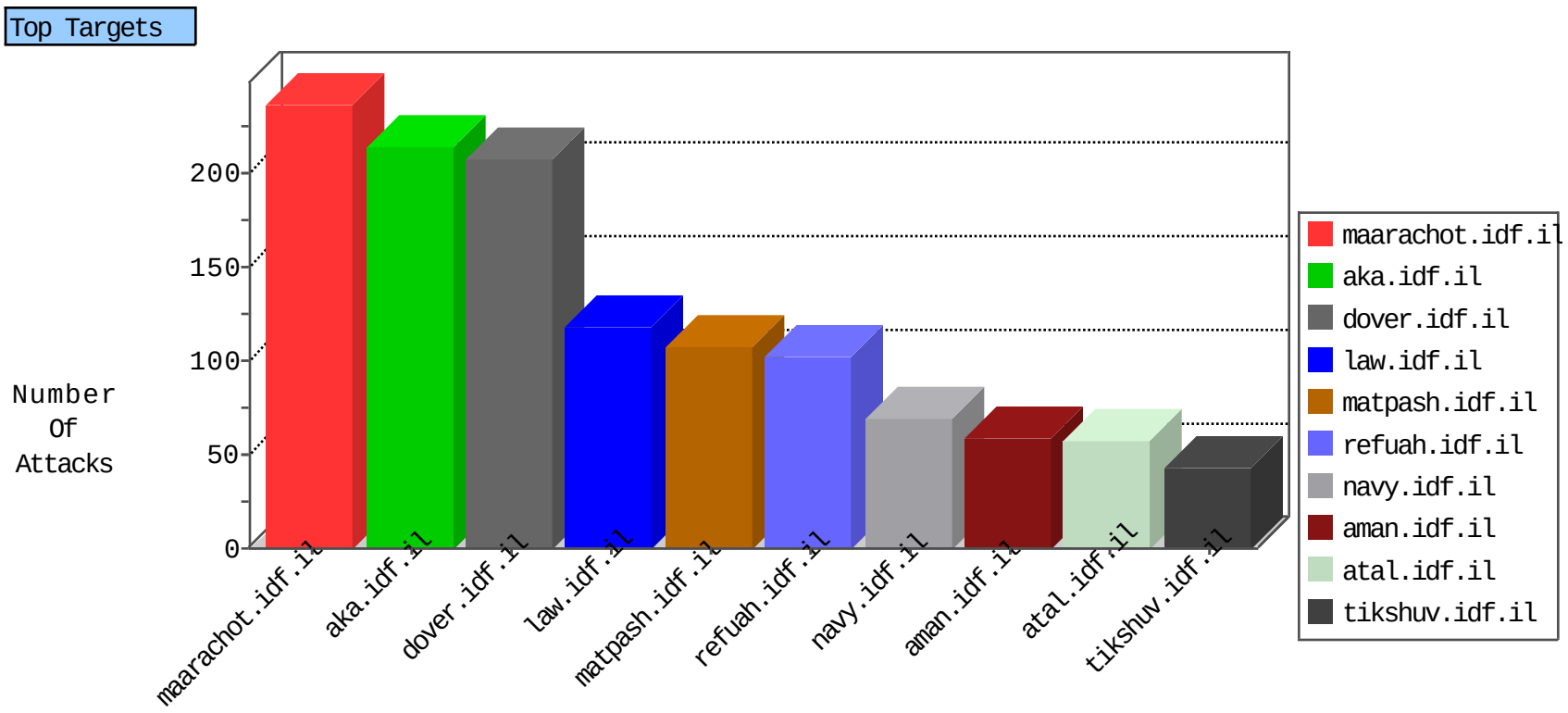
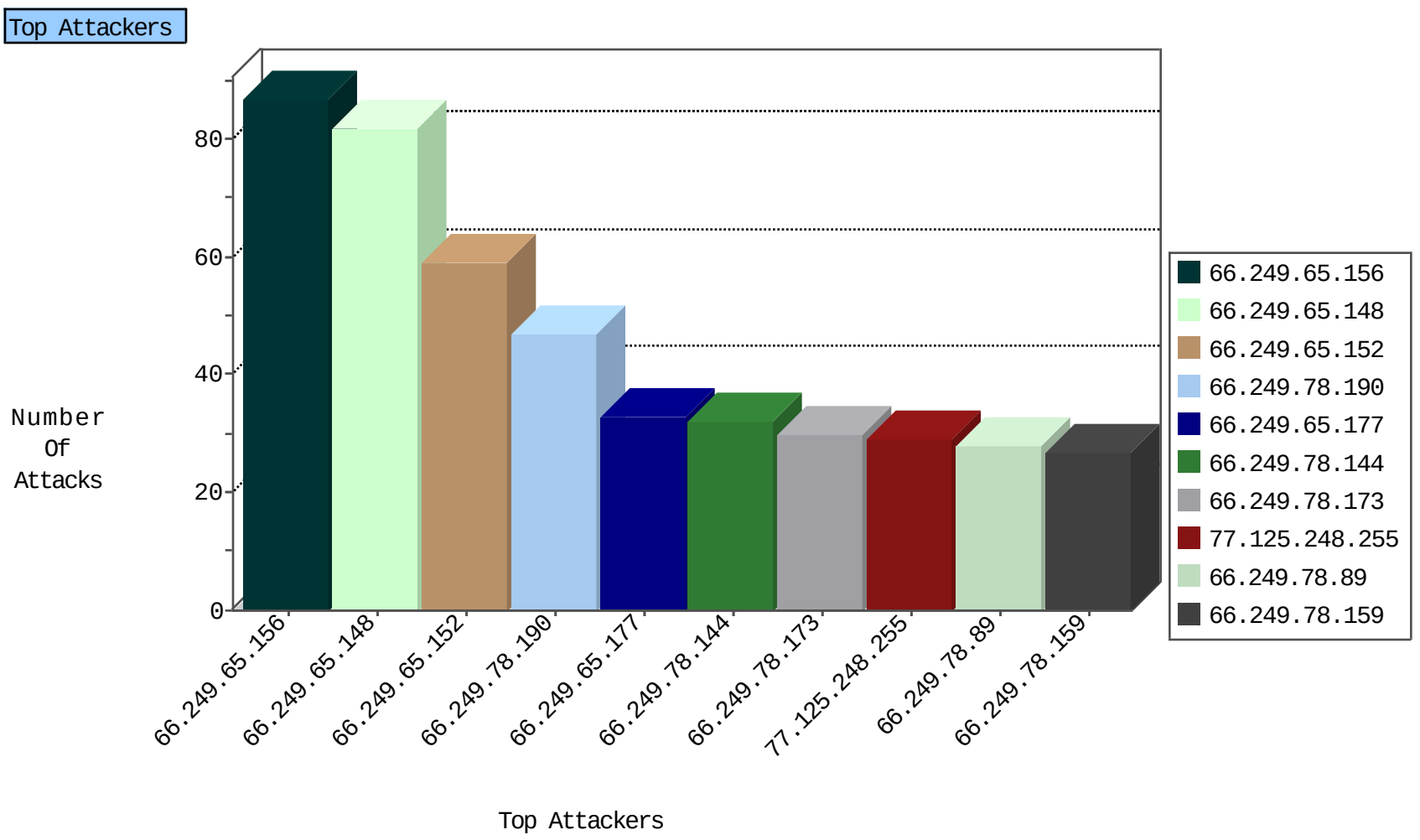
04-05-2015-00:03:02 to 04-05-2015-01:03:02

IDF Under Attack
04-05-2015-00:03:02

Top Targets



Top Attackers



04-05-2015-00:03:02 to 04-05-2015-01:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
77.125.248.255	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	295
82.80.159.29	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	96
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	87
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	82
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	59
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	47
66.249.65.177	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	33
66.249.78.144	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	32
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	30
66.249.78.89	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	28
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	27
66.249.79.42	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	22
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	22
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	22
66.249.78.96	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	20
66.249.78.146	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	20
66.249.65.173	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	20
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	18
66.249.78.153	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	18
66.249.78.160	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	18
66.249.65.181	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	16
66.249.78.130	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	16
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	14
66.249.78.2	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	13
66.249.78.137	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	12
66.249.79.34	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	12
66.249.81.136	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	11
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	11
66.249.79.124	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	10
66.249.79.71	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	10
66.249.64.49	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	10
66.249.78.228	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	9
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	9
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.93.131	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	8
66.249.78.148	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	8
66.249.78.61	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	7
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.65.169	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
66.249.65.195	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	7
66.249.79.87	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	7
66.249.79.55	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	7
66.249.81.144	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	6
66.249.79.140	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.81.140	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
66.249.78.215	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	5
66.249.78.222	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	5

04-05-2015-00:03:02 to 04-05-2015-01:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.156	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.117.245.182	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
93.172.0.198	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
198.20.70.114	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_P-N_40-59	Permit	1
178.77.179.21	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
5.29.202.22	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.76.176	test.ncore.idf.il	DVRep_P-N_40-59	Permit	1
46.120.55.253	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
37.26.146.216	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.77.178	e.matpash.idf.il	DVRep_P-N_40-59	Permit	1
89.139.182.210	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.35	akaws.idf.il	DVRep_P-N_40-59	Permit	1
46.19.85.236	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-05-2015-00:03:02 to 04-05-2015-01:03:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
87.69.162.253	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.186.37.233	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.246.140.120	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.77.179	e.mazi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
52.5.23.174	United States	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
218.27.204.27	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
46.19.86.231	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
188.138.9.51	Germany	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
177.85.235.107	Brazil	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
128.199.254.26	Singapore	147.237.72.166	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
119.97.231.102	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.67	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
52.5.23.174	United States	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
218.27.204.27	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
52.5.23.174	United States	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -f -sS	1
177.85.235.107	Brazil	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
177.85.235.107	Brazil	147.237.76.177	ncore.idf.il	ET SCAN NMAP -f -sS	1
119.97.231.102	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 4096	1

04-05-2015-00:03:02 to 04-05-2015-01:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	18
81.230.30.190	Sweden	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	17
85.130.129.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
109.253.135.94	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
176.12.145.36	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
85.130.174.60	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
77.235.134.251	Lebanon	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	8
85.130.129.37	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
185.32.176.98	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	5
185.32.176.98	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
185.32.176.98	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
2.52.147.89	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
109.253.128.88	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
46.19.86.131	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
2.52.147.89	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
37.142.33.127	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.86.208	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
207.46.13.16	United States	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	2
109.253.142.241	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
5.102.254.32	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.85.67	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.85.11	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
176.228.214.4	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.19.85.11	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
8.37.227.70	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	2
46.19.86.28	Israel	147.237.0.19	madim.atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.161	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
37.142.33.127	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
5.9.97.92	Germany	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
80.246.136.211	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
46.19.86.194	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.34	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.90	United States	147.237.77.227	e.hamaz.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
80.246.130.4	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
188.138.17.205	France	147.237.8.28	e.mobile-ks.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.86.73	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
173.199.65.38	Canada	147.237.8.28	e.mobile-ks.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
109.253.142.241	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
5.29.76.35	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.67	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
141.212.122.154	United States	147.237.76.147	chinuch.aka.idf.il		drop	drop	1
8.37.228.77	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
80.246.130.4	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.86.88	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
37.142.188.230	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
62.0.76.227	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.154	United States	147.237.77.227	e.hamaz.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
8.37.228.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1

04-05-2015-00:03:02 to 04-05-2015-01:03:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.180.33.171	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	23
176.228.214.4	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
93.172.16.160	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
77.127.149.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
84.111.210.116	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
5.29.77.162	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
77.127.149.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
37.8.114.242	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
114.112.90.54	China	147.237.76.30	himush.idf.il	Unauthorized HTTP Method	Block	1
84.228.118.117	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
46.121.86.159	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
207.46.13.16	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13606-he/dover.aspx×³Ã–×³Â?"×³Ö³Æ'Ö¶â€™Ö³â€ ×'â‚¬â„¢Ö³Æ'×'â‚¬Âš Ö³â€šÖ²Â¯Ö³Æ'Ö¶â€™Ö³Â¢×'â€šÂ¬ÖµÂ¡Ö³Æ'×'â‚¬Âš Ö³â€šÖ²Â¿Ö³Æ'Ö¶â€™Ö³Â¢×'â€šÂ¬ÖµÂ¡Ö³Æ'×'â‚¬Âš Ö³â€šÖ²Â½	Block	1
109.253.133.99	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/history/degania.stm	Block	1
85.250.111.119	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
70.167.8.44	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0926-1.stm	Block	1
212.76.97.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
109.253.141.24	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.180.33.171	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0212-2.stm	Block	1
89.138.202.125	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
212.76.114.250	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
109.253.149.204	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.111.103.183	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
188.165.15.198	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.198	Block	1
110.85.94.47	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/grapheat.stm	Block	1
37.26.148.255	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/rus	Block	1
203.133.169.157	Korea, Republic of	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 203.133.169.157	Block	1
109.253.128.88	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.176.181.226	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

04-05-2015-00:03:02 to 04-05-2015-01:03:02