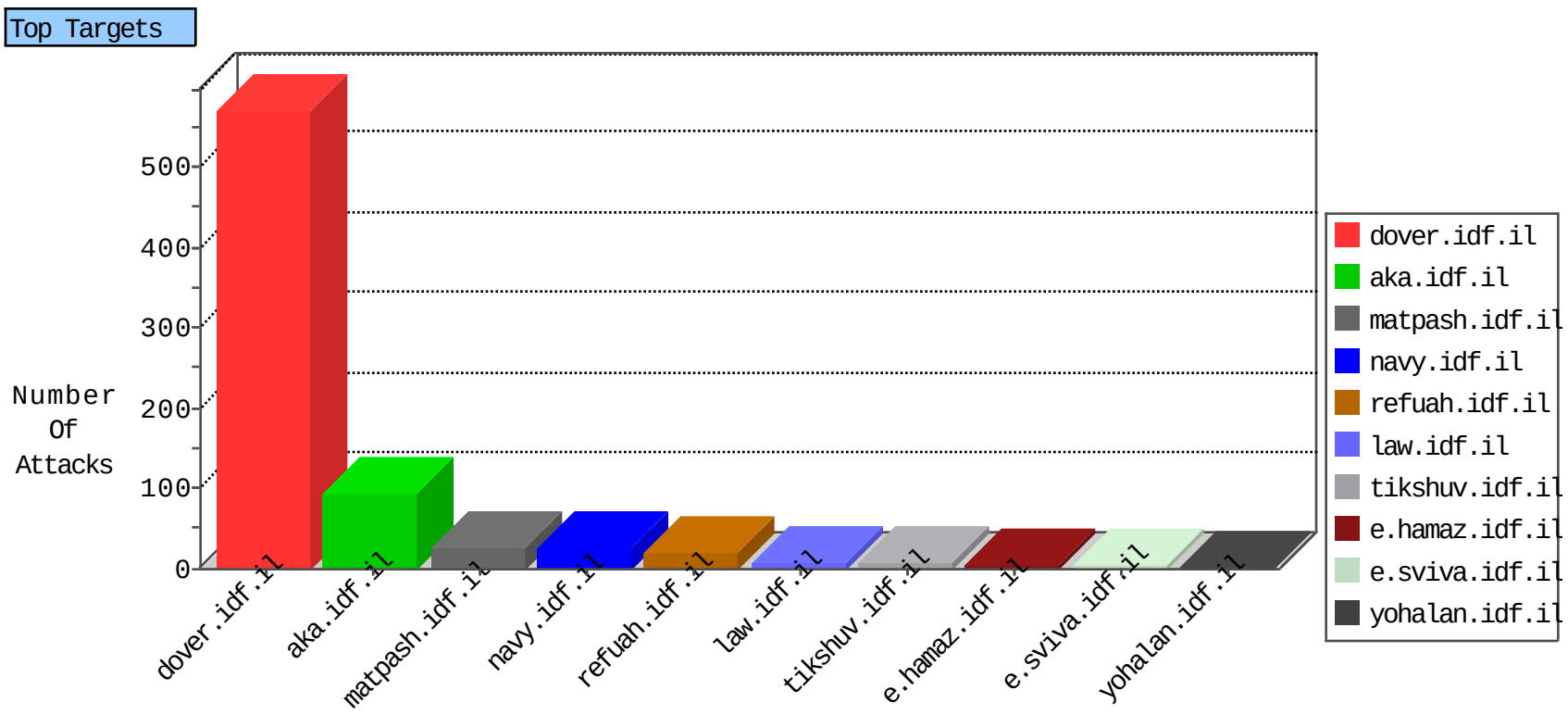
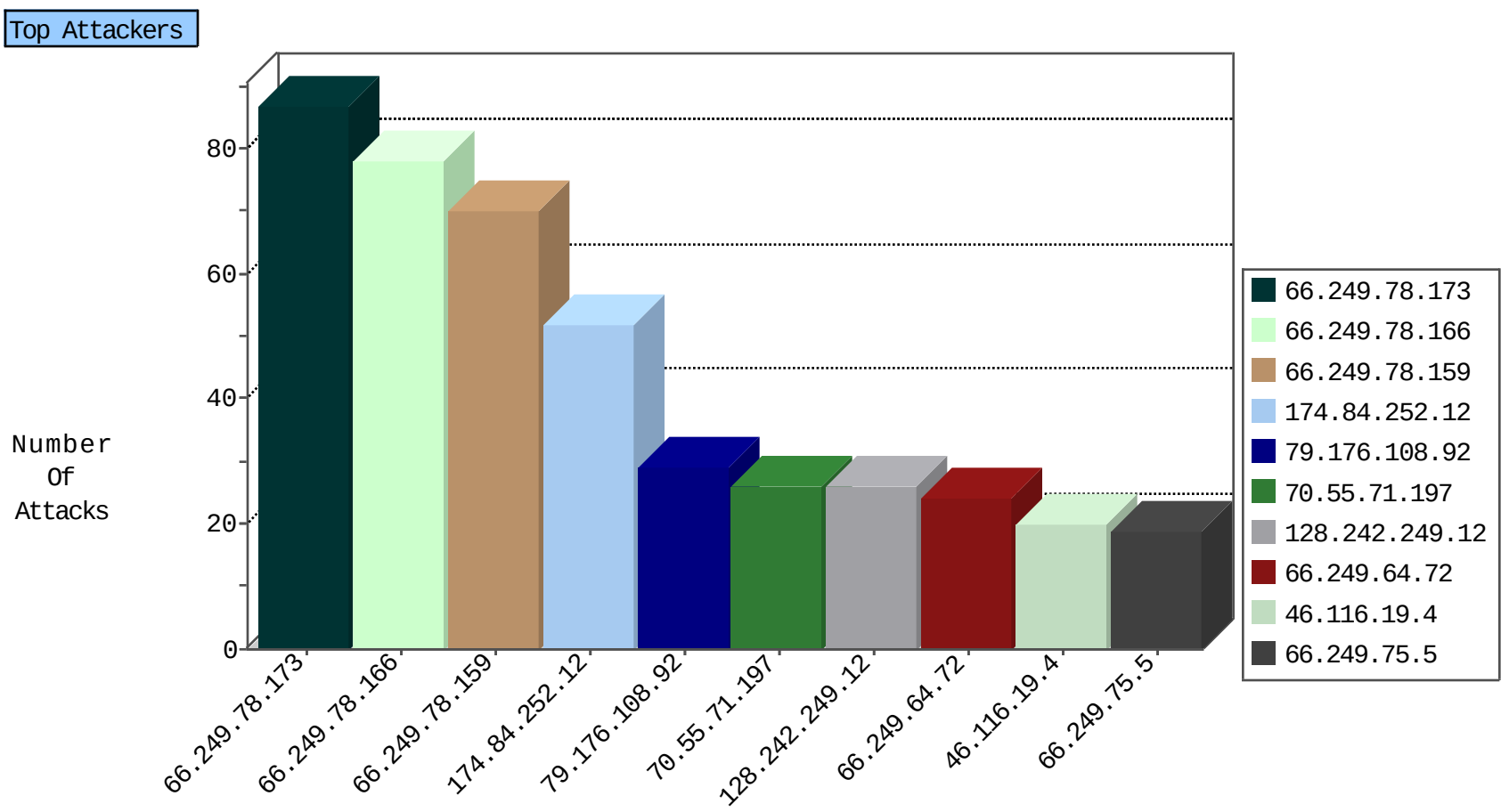
05-01-2015-04:03:05 to 05-01-2015-05:03:05

IDF Under Attack
05-01-2015-04:03:05

Top Targets



Top Attackers



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

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.64.66	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3638
66.249.64.2	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	750
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
204.42.253.2	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2
27.254.96.52	Thailand	147.237.76.196	e.sviva.idf.il	JLM_Purple_Con_Limit_Http	drop	1
107.154.64.10	United States	147.237.77.227	e.hamaz.idf.il	L4 Source or Dest Port Zero	drop	1

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	26
95.173.170.238	Turkey	147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	3
95.173.170.238	Turkey	147.237.72.166	aka.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	2
66.240.236.119	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	2
71.6.165.200	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.148	gqcenter.aka.idf.i	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1

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

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
95.173.170.238	Turkey	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	2
80.246.130.114	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.154	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
218.77.79.43	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
218.60.48.57	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
119.90.139.71	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
218.60.48.57	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.165	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
201.239.118.143	Chile	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.165	Japan	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
119.90.139.71	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.165	Japan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
119.90.139.71	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -f -sS	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.224.132.118	Russian Federation	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
174.84.252.12	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
79.176.108.92	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
70.55.71.197	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
46.116.19.4	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
46.19.85.170	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	18
66.249.75.13	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
203.100.0.82	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
66.249.75.5	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
45.37.124.166		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
66.249.75.117	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
157.55.39.176	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
213.5.154.122	Switzerland	147.237.77.216	dover.idf.il	SAM rule	drop	drop	6
41.185.12.165	South Africa	147.237.77.216	dover.idf.il	SAM rule	drop	drop	6
157.55.39.138	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.19.86.207	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.86.207	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.98.158.199	Ukraine	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.78.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.249.64.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
65.19.138.33	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.64.76	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
130.211.117.114		147.237.77.216	dover.idf.il	Web Servers Slow HTTP Denial of Service	Web Server Enforcement Violation	reject	2
23.29.122.195	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.3	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
185.32.177.193	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
32.138.32.53	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.92	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
69.120.132.123	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
77.237.138.202	Czech Republic	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	2
157.55.39.204	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
184.173.183.174	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
50.138.138.55	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
32.215.196.49	United States	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
71.209.40.26	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
185.32.177.193	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
66.249.64.18	Israel	147.237.0.19	madim.atal.idf.i	SAM rule	drop	drop	1
157.55.39.177	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
85.65.188.161	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
174.84.252.12	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
50.138.138.55	United States	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	70
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	65
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	40
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	29
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	18
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.72	Block	16
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.76	Block	13
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.197	Block	7
66.249.75.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.190	Block	6
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	6
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	4
66.249.64.136	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.64.136	Block	4
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	4
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.204	Block	4
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.92	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.75.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_text.asp	Block	2
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	2
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19519-he/kkkkkkk=af034308kkkkkkk_af034308	Block	1
66.249.78.140	Israel	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on tikshuv.idf.il//main/giyus/general.aspx	Block	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.92	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.132	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/edim/yoman/yoman.asp	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/iaf/669.stm	Block	1
66.249.78.161	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/history/degania.stm	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.80	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/templates/sendtofriend/sendtofriend.aspx	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.3	Block	1
66.249.75.5	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.75.5	Block	1
180.76.6.21	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0113-1.stm	Block	1
66.249.78.147	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.48	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/mobile/	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.204	Block	1
66.249.78.87	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/1319-he/hamaz.aspx	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.147	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/yohalan/forums/asp/showforum.asp	Block	1
184.105.247.195	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catlD in www.aka.idf.il/yohalan/main/main.asp	None	1
66.249.67.73	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/mobile/	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
66.249.78.120	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/general.aspx	Block	1
66.249.75.26	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
207.46.13.20	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/giyus/general.aspx	Block	1

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