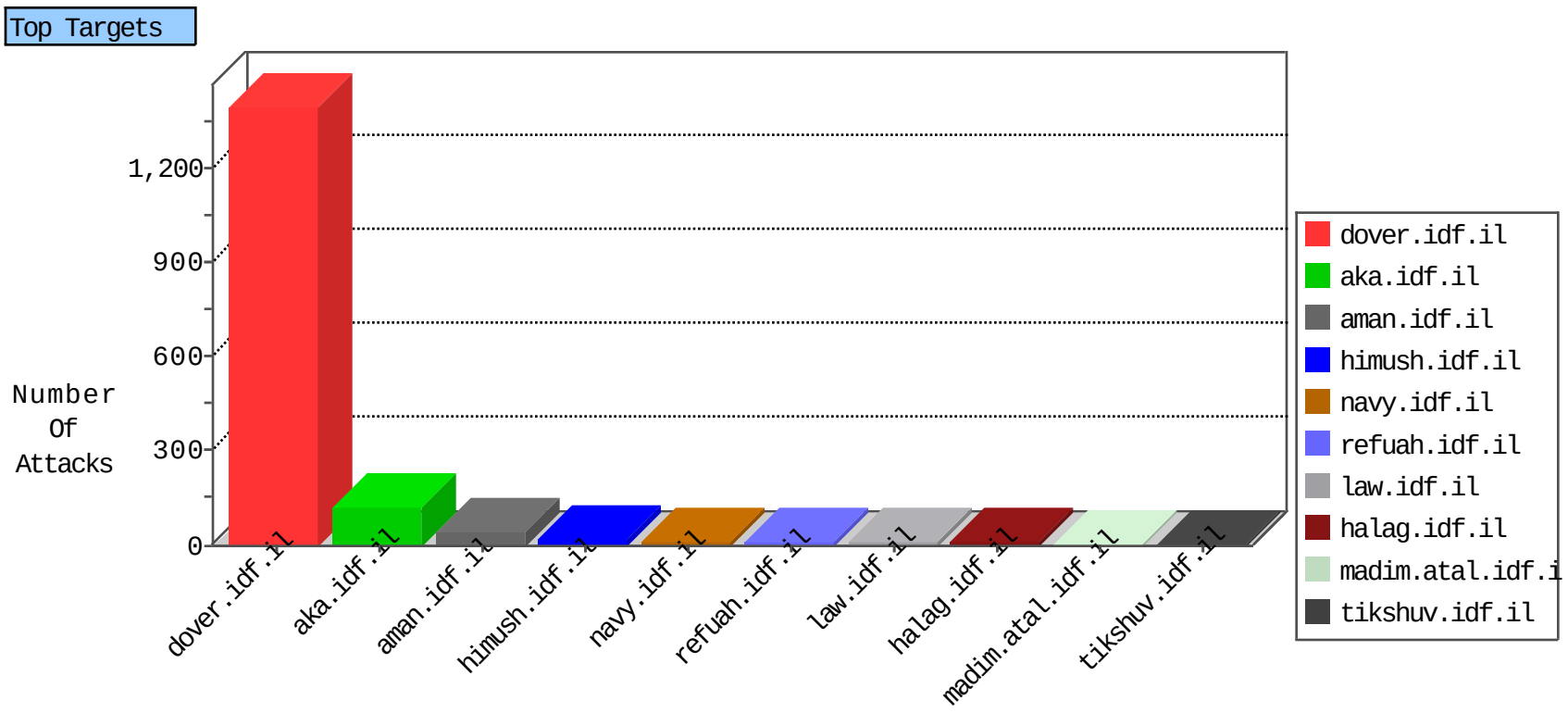
05-01-2015-19:03:09 to 05-01-2015-20:03:09

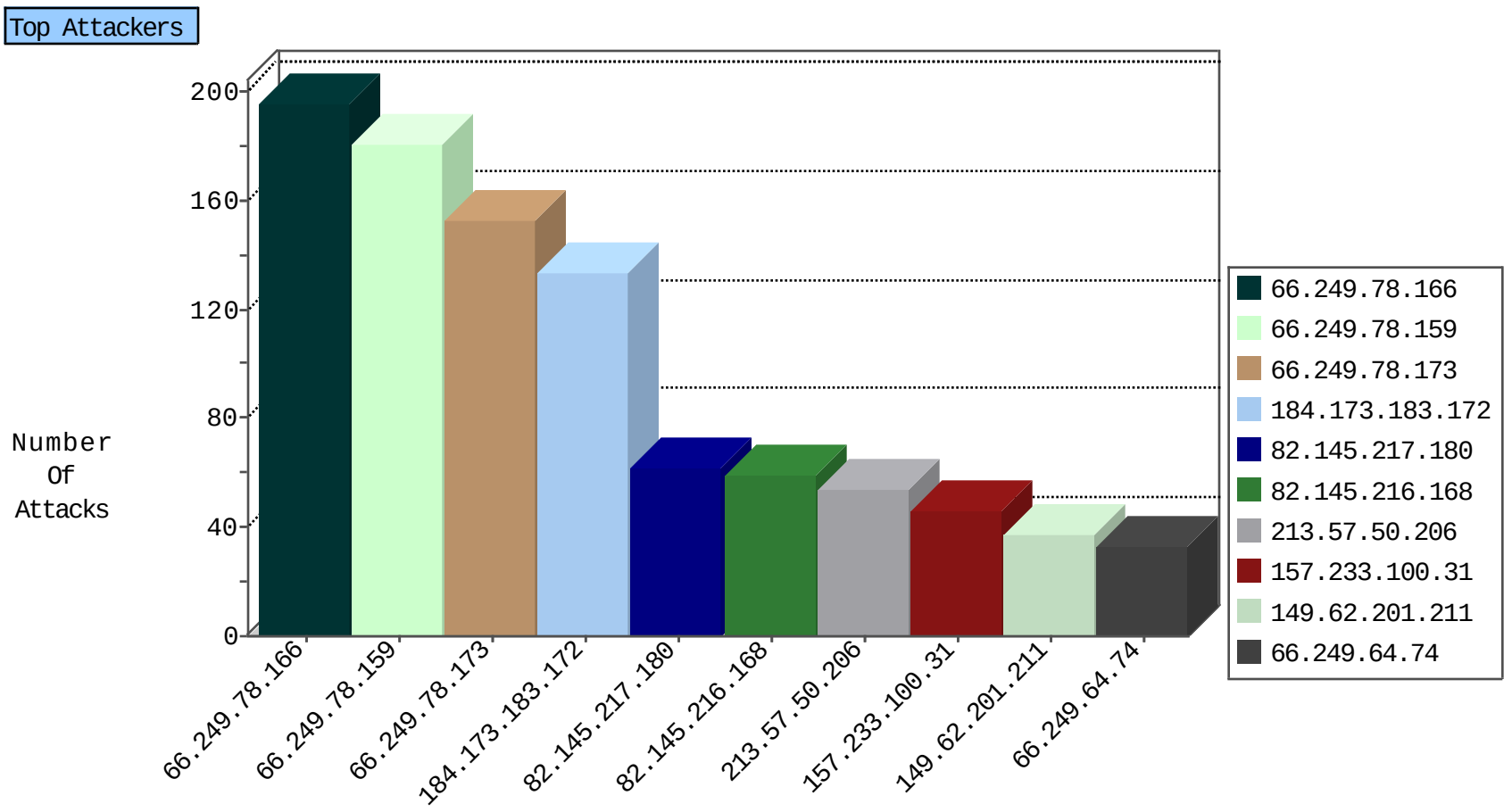
IDF Under Attack
05-01-2015-19:03:09

Top Targets



Top Target

Top Attackers



Top Attackers

05-01-2015-19:03:09 to 05-01-2015-20:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5764
85.250.58.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	259
220.181.108.90	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	163
220.181.108.116	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	113
46.116.216.71	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
2.54.139.176	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.86.76	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
134.147.203.115	Germany	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
2.54.139.176	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
84.228.228.252	Bulgaria	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
93.172.135.253	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
71.6.216.55	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
80.82.78.10	Netherlands	147.237.72.167	ishurim.aka.idf.il	Invalid L4 Header Length	drop	1
2.54.25.91	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
89.176.223.89	Czech Republic	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
89.176.223.89	Czech Republic	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

05-01-2015-19:03:09 to 05-01-2015-20:03:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	134
87.68.10.26	Israel	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
168.170.202.170	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
46.120.206.43	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
46.121.146.32	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.77.179	e.mazi.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
188.138.9.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.35	akaws.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
85.65.202.34	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.236.119	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1

05-01-2015-19:03:09 to 05-01-2015-20:03:09

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	4
46.120.22.12	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
91.224.132.118	Russian Federation	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
218.6.132.45	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.78.173	United States	147.237.77.216	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	1
213.210.205.2	Saudi Arabia	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.66	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
195.3.144.109	Latvia	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack	1
178.32.251.100	France	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
115.69.247.92	India	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
111.73.45.231	China	147.237.76.86	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
101.226.2.99	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -f -sS	1
222.69.94.13	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.132.118	Russian Federation	147.237.72.156	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.6.132.45	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
81.91.219.236	Czech Republic	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
218.6.132.45	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.67	China	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
195.3.144.109	Latvia	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Rapid POP3S Connections - Possible Brute Force Attack	1
148.251.234.20	Germany	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
115.69.247.92	India	147.237.76.177	ncore.idf.il	ET SCAN NMAP -f -sS	1
101.226.2.99	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 2048	1
222.69.94.13	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 3072	1
91.224.132.118	Russian Federation	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
221.229.166.28	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1

05-01-2015-19:03:09 to 05-01-2015-20:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.145.217.180	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	62
82.145.216.168	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	59
213.57.50.206	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	54
157.233.100.31	United States	147.237.77.216	dover.idf.il	TCP segment out of maximum allowed sequence. Packet dropped.	Streaming Engine: TCP Segment Limit Enforcement	drop	41
149.62.201.211	Bulgaria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
89.138.202.88	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.78.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
46.116.216.71	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
80.246.133.181	Israel	147.237.76.30	himush.idf.il	Invalid ACK number	Bad TCP sequence	monitor	11
89.138.8.174	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	10
79.183.70.54	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
46.19.86.53	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
85.250.243.0	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
85.250.243.0	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
149.78.102.58	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
80.162.72.66	Denmark	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
46.19.85.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
213.57.28.9	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
46.19.85.191	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
93.173.235.97	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
213.57.28.9	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	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
74.174.236.84	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
186.4.31.150	Costa Rica	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
109.64.170.227	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
5.28.162.18	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.19.85.191	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
157.233.100.31	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.116.29.104	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
71.74.119.139	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
186.4.31.150	Costa Rica	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
109.64.170.227	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
46.19.85.191	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
81.65.188.83	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.116.29.104	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
176.12.147.69	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
80.246.133.181	Israel	147.237.76.30	himush.idf.il	Invalid ACK number	Bad TCP sequence	alert	5
132.69.201.27	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
84.228.58.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
176.12.147.69	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
93.172.135.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5

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	116
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	56
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	47
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	45
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	41
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	41
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	38
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.72	Block	16
213.57.9.227	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.57.9.227	Block	15
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	12
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	10
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	8
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.76	Block	7
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	6
157.55.39.53	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 157.55.39.53	Block	6
84.228.32.79	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	6
85.65.202.34	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	5
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	4
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
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	3
84.111.216.70	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	3
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.186.24.2	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
149.78.22.141	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.183.122.149	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/print_text.asp	Block	2
207.46.13.101	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.101	Block	2
185.53.44.200		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//chinuch/printpreview/	Block	2
66.249.64.77	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/m/	Block	2
66.249.78.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/320-he/patzar.aspx	Block	1
185.53.44.201		147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/228-he/faq.aspx	Block	1
66.249.69.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
185.53.44.85		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//kamlar/printpreview/	Block	1
85.64.179.194	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.228	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/m/	Block	1
66.249.64.73	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//m/	Block	1
185.53.44.44		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/golani/golani3.stm	Block	1
94.153.9.66	Ukraine	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
66.249.78.44	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/mobile/	Block	1
185.53.44.124		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//kamlar/printpreview/	Block	1
185.53.44.61		147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/eurl.axd/7b2f3488d4aa87438d24d91e7db09bef/	Block	1
46.229.164.113	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/trajector	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Double URL Encoding - parameter: pic in www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
213.57.9.227	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	1
66.249.78.125	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/870-he/patzar.aspx	Block	1
185.53.44.202		147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/brothers/faq/	None	1
157.55.39.46	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/012804-1.stm	Block	1
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: catid%5Cu003d59336 in www.aka.idf.il/main/giyus/general.aspx	Block	1

05-01-2015-19:03:09 to 05-01-2015-20:03:09