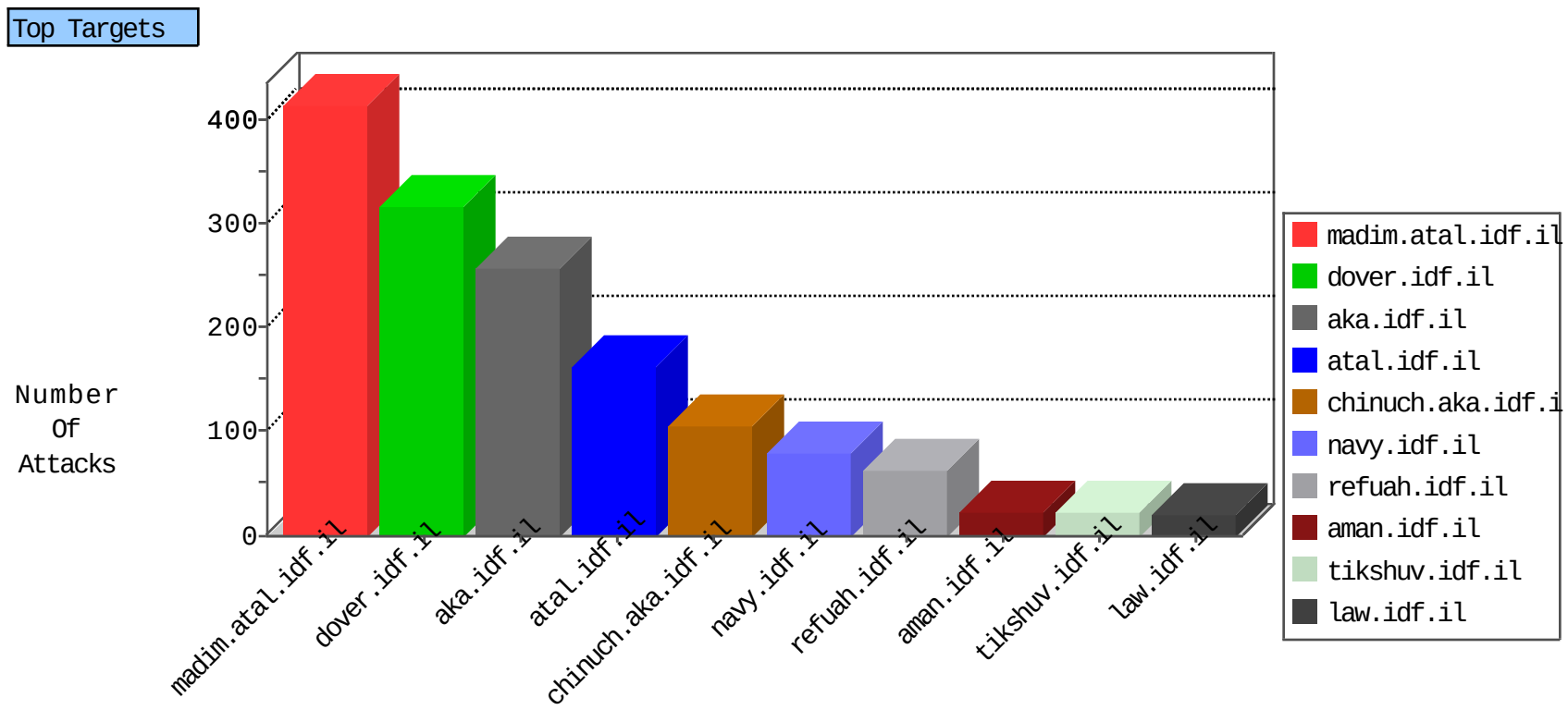
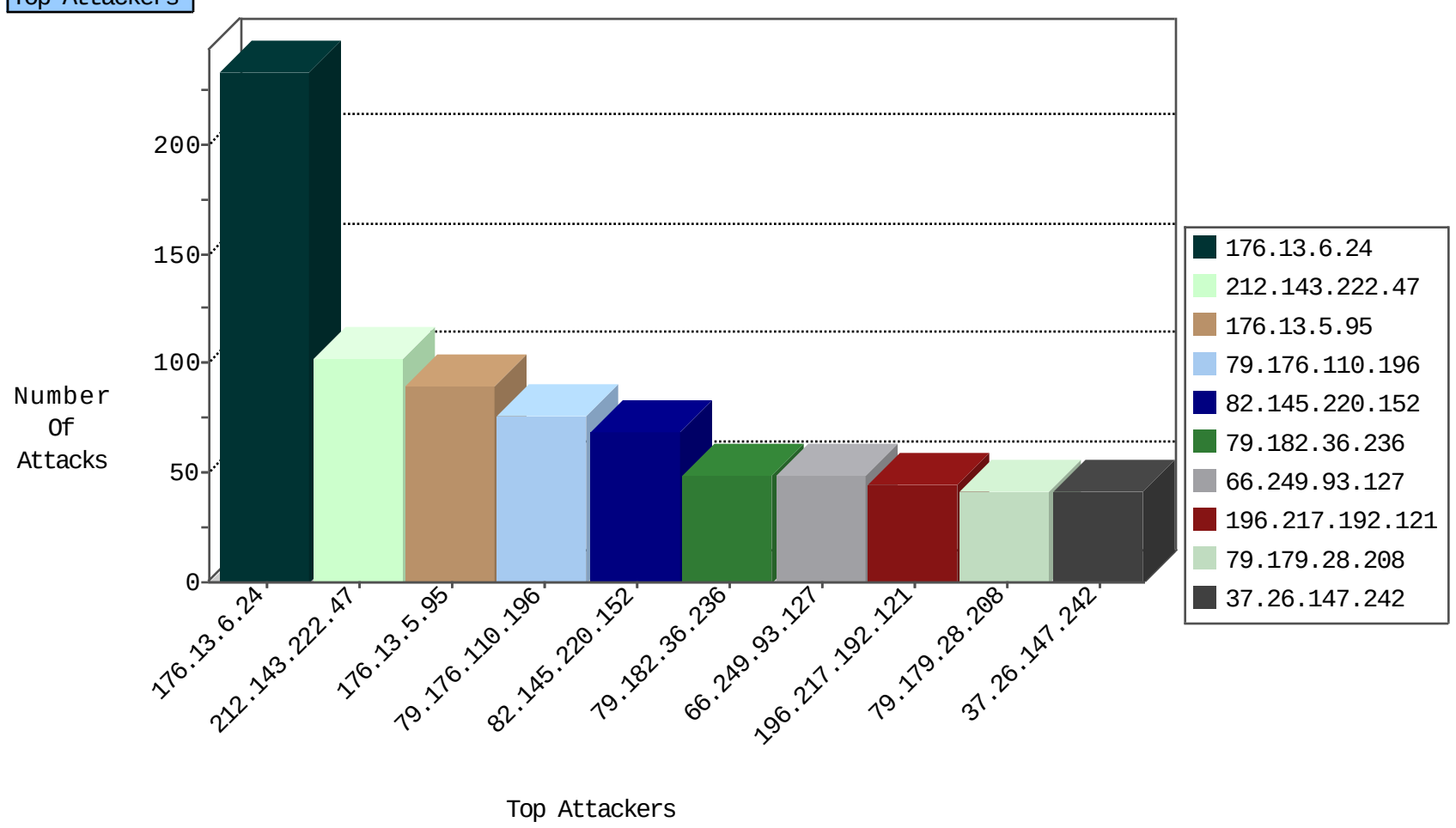
03-07-2016-23:04:04 to 03-08-2016-00:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-07-2016-23:04:04 to 03-08-2016-00:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.220.152	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	69
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
79.178.125.211	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
79.178.125.211	Israel	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	3
85.25.43.94	Germany	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets_Con_Limit	drop	2
185.35.62.149	Switzerland	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
193.222.63.122	Romania	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.114	Switzerland	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
198.48.92.104	United States	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.144	Switzerland	147.237.77.178	e.matpash.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.44	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
198.48.92.104	United States	147.237.72.14	dover.idf.il(old)	Block_Udp_All_Nets	drop	1

03-07-2016-23:04:04 to 03-08-2016-00:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.189.37	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
41.185.31.40	South Africa	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
216.201.148.210	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
66.249.69.95	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
94.23.19.178	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
2.54.25.156	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.109	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.159	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
109.64.188.175	Israel	147.237.72.166	aka.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-07-2016-23:04:04 to 03-08-2016-00:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.185.31.40	147.237.77.74	South Africa	law.idf.il	SQL Injection - Select From	6
216.201.148.210	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.102.9.10	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
193.201.227.120	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN Potential SSH Scan	1
187.35.169.150	147.237.8.27	Brazil	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.252.84	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
183.60.48.25	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
98.119.105.221	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -f -sS	1
218.246.0.97	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
61.244.49.137	147.237.77.226	Hong Kong	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
194.187.249.70	147.237.76.86	Europe	navy.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
189.218.151.126	147.237.8.14	Mexico	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.52.157.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.252.84	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
183.60.252.84	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
105.154.192.163	147.237.77.233	Morocco	atal.idf.il	ET SCAN NMAP -sS window 4096	1
98.119.105.221	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
61.244.49.137	147.237.72.14	Hong Kong	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1

03-07-2016-23:04:04 to 03-08-2016-00:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.143.222.47	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	102
66.249.93.127	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	49
79.182.36.236	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	48
196.217.192.121	Morocco	147.237.77.216	dover.idf.il	drop		drop	43
79.179.28.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	22
181.114.135.87	Argentina	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	16
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
66.249.93.67	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	12
89.139.255.143	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
87.68.250.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
188.120.148.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.176.54.126	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.86.87	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.195	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
85.250.215.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.251	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.147.242	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.0	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.120.156.245	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.242	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
5.22.135.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.147.242	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.0	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.46.39.169	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.242	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
89.139.255.143	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.176.175.14	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.242	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.195	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.3.144.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.142.146	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
79.182.212.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.139.255.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
87.70.54.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.186.48.150	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
37.26.147.242	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
132.74.150.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
37.26.147.242	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
37.26.149.222	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.87	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.242	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.46.41.182	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.242.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
78.95.97.187	Romania	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	5
46.19.85.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.6.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	234
176.13.5.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
79.176.110.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
5.29.123.133	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.29.123.133	Block	11
2.54.27.123	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
80.246.136.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.192	Israel	147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	4
24.45.172.19	United States	147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.139.157.127	Israel	147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	2
188.120.148.112	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
5.29.41.7	Israel	147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	2
213.8.204.63	Israel	147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	2
185.3.146.101	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
185.120.125.56		147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	2
195.154.173.103	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	2
109.66.17.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.123.133	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx	Block	2
79.181.165.227	Israel	147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	2
5.29.150.250	Israel	147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	2
185.120.126.10		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.177.116.214	Israel	147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	1
173.252.90.231	United States	147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.163	United States	147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	1
46.120.169.97	Israel	147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	1
94.230.93.101	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
78.95.97.187	Romania	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
142.167.75.64	Canada	147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	1
52.37.173.158	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp-login.php	Block	1
89.139.177.173	Israel	147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	1
24.120.54.20	United States	147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	1
192.157.245.13	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/pricing	Block	1
79.178.0.211	Israel	147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	1
51.254.44.137	United Kingdom	147.237.77.234	halag.idf.il	Unauthorized URL Access to /	Block	1
94.230.93.104	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.108.66.198	Israel	147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	1
217.132.55.244	Israel	147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	1
79.176.41.200	Israel	147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	1
149.88.205.189	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
65.55.210.143	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
89.139.255.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.178.114.153	Israel	147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.3	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
52.0.19.0	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17212-en/dover.aspxconfirms	Block	1
84.108.210.178	Israel	147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	1
79.176.54.126	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
185.120.125.88		147.237.76.86	navy.idf.il	Distributed Suspicious Response Code	Block	1
149.88.205.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.3	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/shared/ajax/setivgallerycontrol.aspx	Block	1