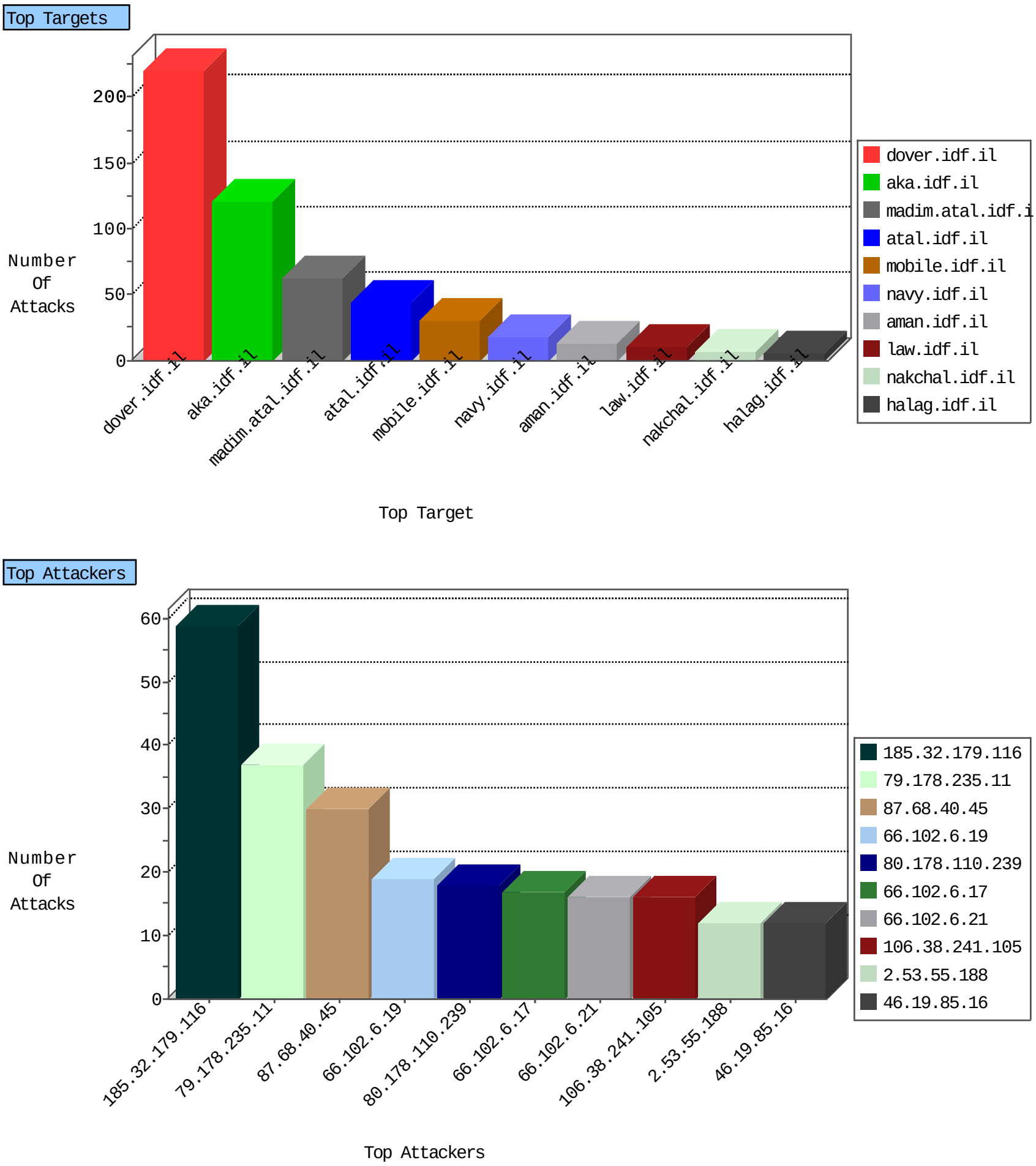
09-16-2016-21:04:03 to 09-16-2016-22:04:03

IDF Under Attack Daily Report



09-16-2016-21:04:03 to 09-16-2016-22:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
157.55.39.128	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.111	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.221	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
160.80.221.37	Italy	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
134.117.226.180	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.13	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
45.35.64.142	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
195.113.161.84	Czech Republic	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
193.1.13.12	Ireland	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-16-2016-21:04:03 to 09-16-2016-22:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.255.51.67	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
149.202.54.34	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-16-2016-21:04:03 to 09-16-2016-22:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
84.93.84.77	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
46.120.122.219	147.237.76.86	Israel	navy.idf.il	Xenu Link Sleuth User Agent	2
109.60.153.178	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.60.153.178	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN NMAP -sS window 1024	1
212.92.127.197	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.10	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.92.127.197	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.12.34.31	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
212.92.127.197	147.237.76.148	Russian Federation	gqcenter.aka.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
46.120.122.219	147.237.76.31	Israel	nakchal.idf.il	Xenu Link Sleuth User Agent	1
202.155.58.28	147.237.76.176	Indonesia	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
116.71.128.85	147.237.0.200	Pakistan	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
109.67.207.21	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	1
109.60.153.178	147.237.76.34	Russian Federation	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.60.153.178	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
212.92.127.197	147.237.77.234	Russian Federation	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.60.153.178	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.92.127.197	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.92.127.197	147.237.76.176	Russian Federation	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.155.58.28	147.237.76.196	Indonesia	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
133.242.4.52	147.237.77.216	Japan	dover.idf.il	ET SCAN NMAP -sS window 1024	1
111.20.131.46	147.237.8.27	China	e.madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.60.153.178	147.237.76.42	Russian Federation	refuah.idf.il	ET SCAN NMAP -sS window 1024	1

09-16-2016-21:04:03 to 09-16-2016-22:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.178.235.11	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
87.68.40.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.102.6.19	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
66.102.6.17	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
66.102.6.21	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
176.13.8.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
84.94.175.154	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.53.55.188	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.253.131.83	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.120	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.178.110.239	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.28.185.108	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
80.178.235.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.53.55.188	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
95.90.240.3	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
80.178.110.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
46.19.85.178	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
95.90.240.3	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
157.55.39.128	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
80.178.235.28	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
109.253.132.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.35	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
114.121.238.231	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.91	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
80.178.110.239	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.178	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.178.235.11	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
80.178.110.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
93.173.3.224	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
106.38.241.105	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
5.29.171.138	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.40.139.39	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
185.20.5.157	United Kingdom	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
79.177.52.138	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
5.28.163.224	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.239	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
178.39.218.11	Switzerland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.64.53.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

09-16-2016-21:04:03 to 09-16-2016-22:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
77.139.31.221	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.116.34.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.6.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.27	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
185.32.179.116	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
84.94.209.30	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/540-he/	Block	1
54.158.62.102	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
157.55.39.44	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
213.8.204.37	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
84.109.38.47	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
2.53.152.185	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
77.237.146.28	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized Method HEAD for /	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus	Block	1
213.8.204.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
99.254.118.43	Canada	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl55 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.65.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
5.29.165.46	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
180.76.15.155	China	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
79.178.235.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
46.120.122.219	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/2/1682.doc	Block	1
109.67.194.215	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.66.24	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/4/424.doc	Block	1
45.79.163.224	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/pratim/pirteyerua/	Block	1
84.94.209.30	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	1
46.121.124.156	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
157.55.39.29	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in aka.idf.il/main/home/default.aspx	None	1

09-16-2016-21:04:03 to 09-16-2016-22:04:03