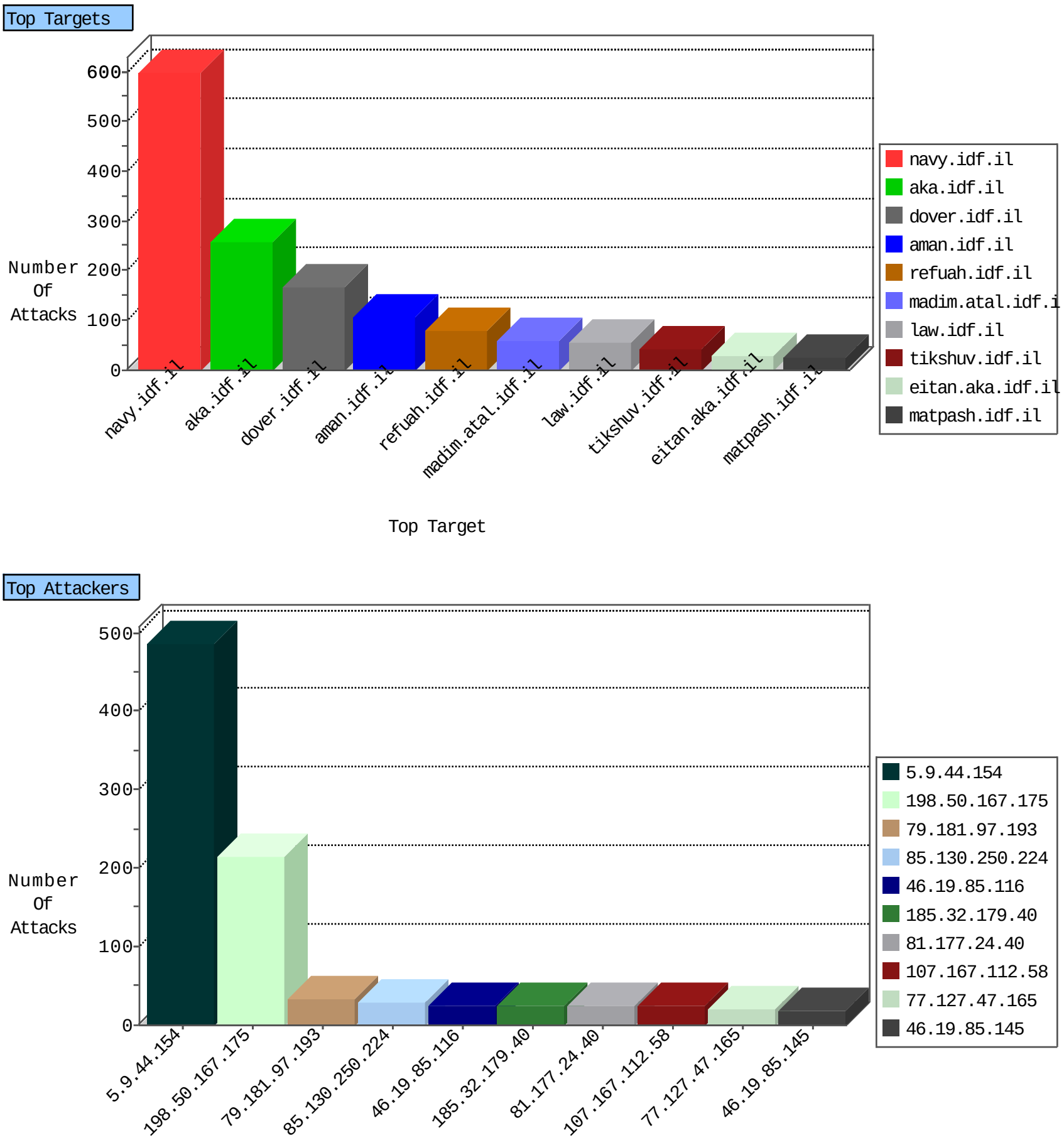
09-11-2016-17:04:01 to 09-11-2016-18:04:01

IDF Under Attack
Daily Report



09-11-2016-17:04:01 to 09-11-2016-18:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	10
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
131.247.2.241	United States	147.237.72.167	ishurim.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
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
123.59.59.52	China	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
193.1.13.14	Ireland	147.237.72.166	aka.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
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
141.226.145.249	Israel	147.237.77.216	dover.idf.il	Black List	drop	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
46.116.19.100	Israel	147.237.72.166	aka.idf.il	Invalid L4 Header Length	drop	1
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.206.158.138	Spain	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
137.132.80.110	Singapore	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
46.116.32.59	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-11-2016-17:04:01 to 09-11-2016-18:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.177.24.40	Russian Federation	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
81.177.24.40	Russian Federation	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
199.58.86.209	United States	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.209	United States	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Permit	1
91.219.122.2	Poland	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
66.240.236.119	United States	147.237.0.16	my-kosher-kravi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
91.219.122.2	Poland	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	1
199.87.254.195	United States	147.237.77.74	law.idf.il	34161: ICMP: Communication with Destination Host is Administratively Prohibited (Code 10)	Block	1
77.67.47.7	France	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
94.102.53.177	Netherlands	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

09-11-2016-17:04:01 to 09-11-2016-18:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.181.97.193	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	33
91.219.122.2	147.237.77.74	Poland	law.idf.il	SQL Injection - Select From	14
81.177.24.40	147.237.77.74	Russian Federation	law.idf.il	SQL Injection - Select From	14
77.67.47.7	147.237.72.166	France	aka.idf.il	SQL Injection - Select From	8
109.60.153.178	147.237.76.38	Russian Federation	e.e.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
211.141.78.56	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
185.19.218.114	147.237.76.38	Germany	e.e.meitav.idf.i	ET SCAN NMAP -sS window 4096	1
46.227.67.158	147.237.0.35	Sweden	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.77.243	United Kingdom	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
5.28.142.196	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.226.40.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.60.153.178	147.237.76.86	Russian Federation	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
95.152.80.48	147.237.77.19	Switzerland	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
87.70.40.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.36.54	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.182.151	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.93.185.10	147.237.76.200	Ukraine	eitan.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.66.176	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
185.19.218.114	147.237.76.38	Germany	e.e.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
37.142.233.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.137.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.117.229	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

09-11-2016-17:04:01 to 09-11-2016-18:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack		monitor	334
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	105
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	48
107.167.112.58	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	23
46.19.86.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.120.192.34	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
46.19.85.116	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.145	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
198.50.167.175	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
198.50.167.175	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
100.92.127.126		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
62.0.230.1	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	11
198.50.167.175	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
198.50.167.175	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
198.50.167.175	Canada	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
198.50.167.175	Canada	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
198.50.167.175	Canada	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
198.50.167.175	Canada	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
198.50.167.175	Canada	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
198.50.167.175	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
198.50.167.175	Canada	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
198.50.167.175	Canada	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
198.50.167.175	Canada	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
198.50.167.175	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
198.50.167.175	Canada	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
85.130.250.224	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
198.50.167.175	Canada	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
198.50.167.175	Canada	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.85.116	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
85.130.250.224	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
198.50.167.175	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
198.50.167.175	Canada	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
198.50.167.175	Canada	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.85.109	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
198.50.167.175	Canada	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
198.50.167.175	Canada	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
176.13.18.212	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.13.245.34	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
185.27.106.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
79.183.72.52	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
109.67.14.129	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
176.13.18.212	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
193.43.246.250	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
2.55.179.24	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.52	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.235.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.245.34	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.74	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.228	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
77.139.56.94	France	147.237.72.166	aka.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
77.127.47.165	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	21
46.19.85.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
37.26.148.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
176.13.243.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
109.65.126.200	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	7
85.65.59.213	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	5
2.53.176.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
31.154.81.14	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	4
109.186.76.154	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
46.116.208.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
93.173.19.17	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
79.183.75.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.207.205	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
188.120.154.100	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.249	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method i/601.1 in URL	Block	1
79.183.8.153	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.132.115.49	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
176.13.235.185	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
192.117.134.89	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
109.253.198.149	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
40.77.167.49	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
94.100.237.52	Georgia	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step4.aspx	Block	1
79.178.97.145	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Unknown SSL Session	None	1
192.169.7.223	United States	147.237.76.86	navy.idf.il	Unauthorized Method HEAD for 147.237.76.86/	Block	1
46.120.245.200	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Unknown SSL Session	None	1
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
2.53.4.240	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.66.177	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
176.13.247.15	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
107.167.112.58	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
37.26.146.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.178.97.145	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
199.58.86.209	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
65.55.210.253	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.asmx/getjs	Block	1
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Malformed URL sdch	Block	1
157.55.39.9	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
2.53.18.167	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.69.238.21	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
68.180.228.41	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
46.19.86.249	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
185.32.179.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.147.199	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
79.181.128.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/resource/userfollowresource/create/	Block	1
207.46.13.59	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method e, in URL sdch	Block	1

09-11-2016-17:04:01 to 09-11-2016-18:04:01