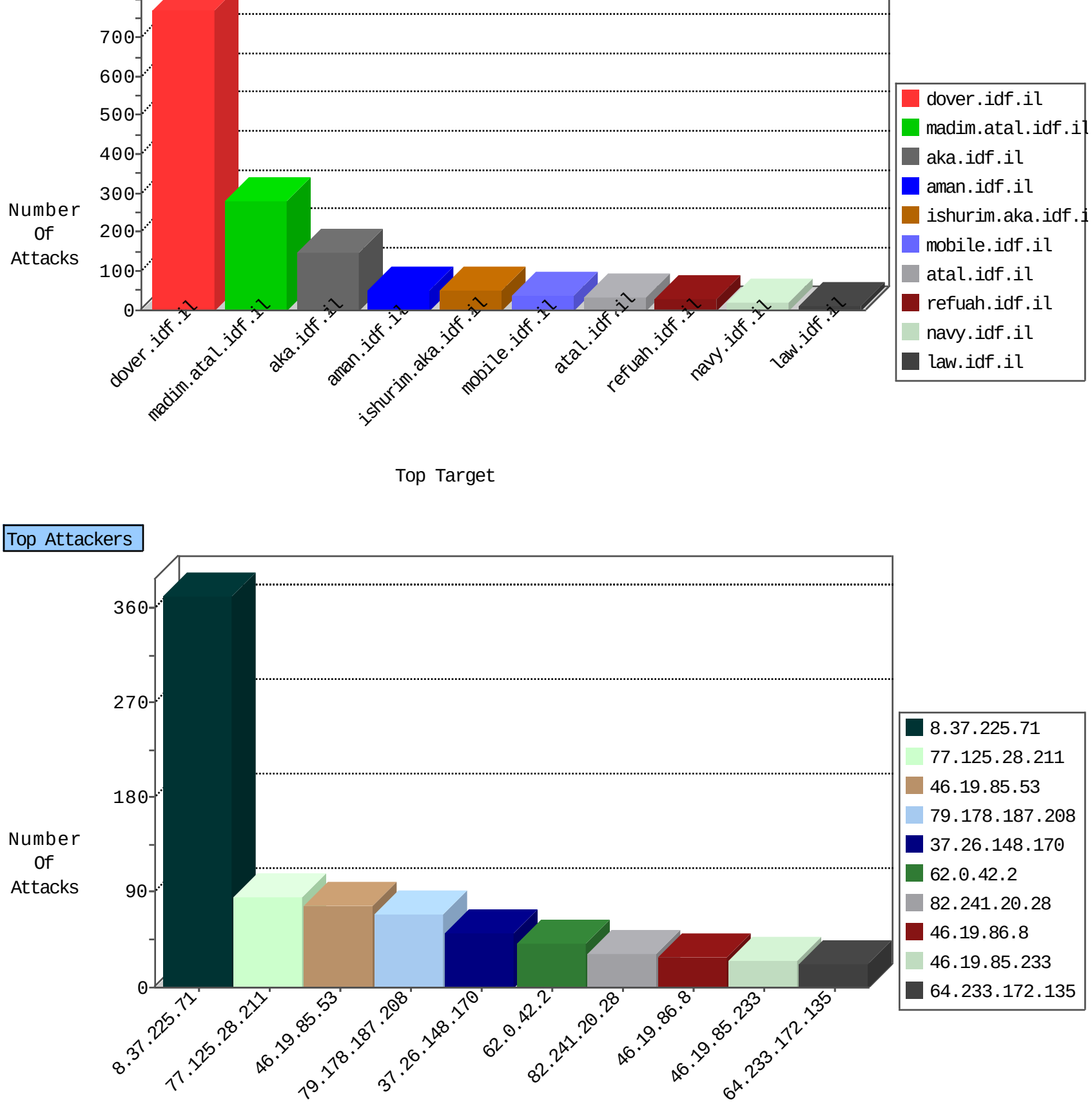
09-04-2016-13:04:01 to 09-04-2016-14:04:01

IDF Under Attack Daily Report



09-04-2016-13:04:01 to 09-04-2016-14:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.51.44	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	109
8.37.225.71	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	6
109.67.167.157	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
46.116.197.11	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
79.178.187.208	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
68.180.230.47	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
217.23.9.123	Netherlands	147.237.76.177	ncore.idf.il	Black List	drop	1
37.142.81.108	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1

09-04-2016-13:04:01 to 09-04-2016-14:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.211.2	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	12
69.30.211.2	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	3
162.210.196.100	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.211.2	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.211	United States	147.237.77.170	maarachot.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.211.2	United States	147.237.76.147	chinuch.aka.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-04-2016-13:04:01 to 09-04-2016-14:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
89.138.148.55	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.24.220	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.116.245.213	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.172.71.251	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.229.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
116.12.175.233	147.237.76.38	Singapore	e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
37.142.226.208	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
116.12.175.233	147.237.76.38	Singapore	e.e.meitav.idf.il	ET SCAN NMAP -f -sS	1
37.26.146.229	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.128.144.131	147.237.8.24	Canada	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
2.55.129.191	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.155	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
219.87.191.219	147.237.76.31	Taiwan	nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
212.179.21.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.44.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
62.219.35.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
178.220.165.231	147.237.76.30		himush.idf.il	ET SCAN NMAP -sS window 1024	1
46.117.82.39	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
161.18.48.241	147.237.77.243	Colombia	mobile.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
45.79.111.169	147.237.77.170	United States	maarachot.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1
116.12.175.233	147.237.76.38	Singapore	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.149.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.228.153	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.195.220	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.159.255.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.155	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-04-2016-13:04:01 to 09-04-2016-14:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
8.37.225.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	219
8.37.225.71	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	147
79.178.187.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
82.241.20.28	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	22
62.0.42.2	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	22
64.233.172.135	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
62.0.42.2	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	19
46.19.86.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
46.19.86.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
2.53.169.146	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.239	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	12
62.0.251.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.105	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	11
5.82.233.68	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
217.194.197.154	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
176.13.227.55	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
109.67.167.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
62.90.81.186	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
81.218.197.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
46.19.85.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.43	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	7
46.19.86.43	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
109.253.240.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.128.199	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.20.252	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.227	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.55.140.20	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.201	Israel	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	6
109.64.34.102	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
109.253.218.24	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
82.241.20.28	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
213.8.204.28	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
46.19.85.227	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
77.239.224.35	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.233	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	5
46.19.85.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.26.148.169	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
100.92.57.67		147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.75	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
109.64.34.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
31.154.81.22	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
46.19.85.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.75	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.43	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
148.177.168.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.228	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
2.55.20.252	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

09-04-2016-13:04:01 to 09-04-2016-14:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.125.28.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	85
46.19.85.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	78
37.26.148.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	51
2.53.13.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
2.55.59.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
46.19.85.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.85.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.86.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.194.164	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.253.194.164	Block	4
82.241.20.28	France	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	4
46.19.86.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.170.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.148.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.32.179.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
77.138.196.78	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	3
46.19.85.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.179.21.194	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	2
77.138.21.142	France	147.237.76.42	refuah.idf.il	Parameter Type Violation searchText in www.refua.atal.idf.il/1653-he/refuah.aspx	Block	2
2.53.169.146	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	2
131.253.27.32	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.194.164	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	2
109.253.209.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	2
65.55.210.180	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.194.164	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	2
131.253.25.178	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for aka.idf.il/	Block	1
2.55.157.116	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.115.97.253	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
66.249.64.219	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1486-he/atal.aspx	Block	1
45.79.111.169	United States	147.237.77.170	maarachot.idf.il	Unknown HTTP Request Method 1 in URL	Block	1
77.139.224.21	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/cityofficers/	Block	1
199.30.25.3	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
212.179.155.129	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
77.138.102.230	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.248	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1316-he/אגף הטכנולוגיה והלוג'סטיקה.aspx	Block	1
192.115.97.253	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 192.115.97.253	Block	1
79.178.118.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1129-he/dover.aspx	Block	1
207.46.13.90	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.36	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.43	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
84.94.97.137	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/7/size338x0/1777.jpg	Block	1
77.138.111.230	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
66.249.66.24	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
192.115.248.2	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1247-he/atal.aspx	Block	1
79.178.178.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
2.53.170.196	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1

09-04-2016-13:04:01 to 09-04-2016-14:04:01