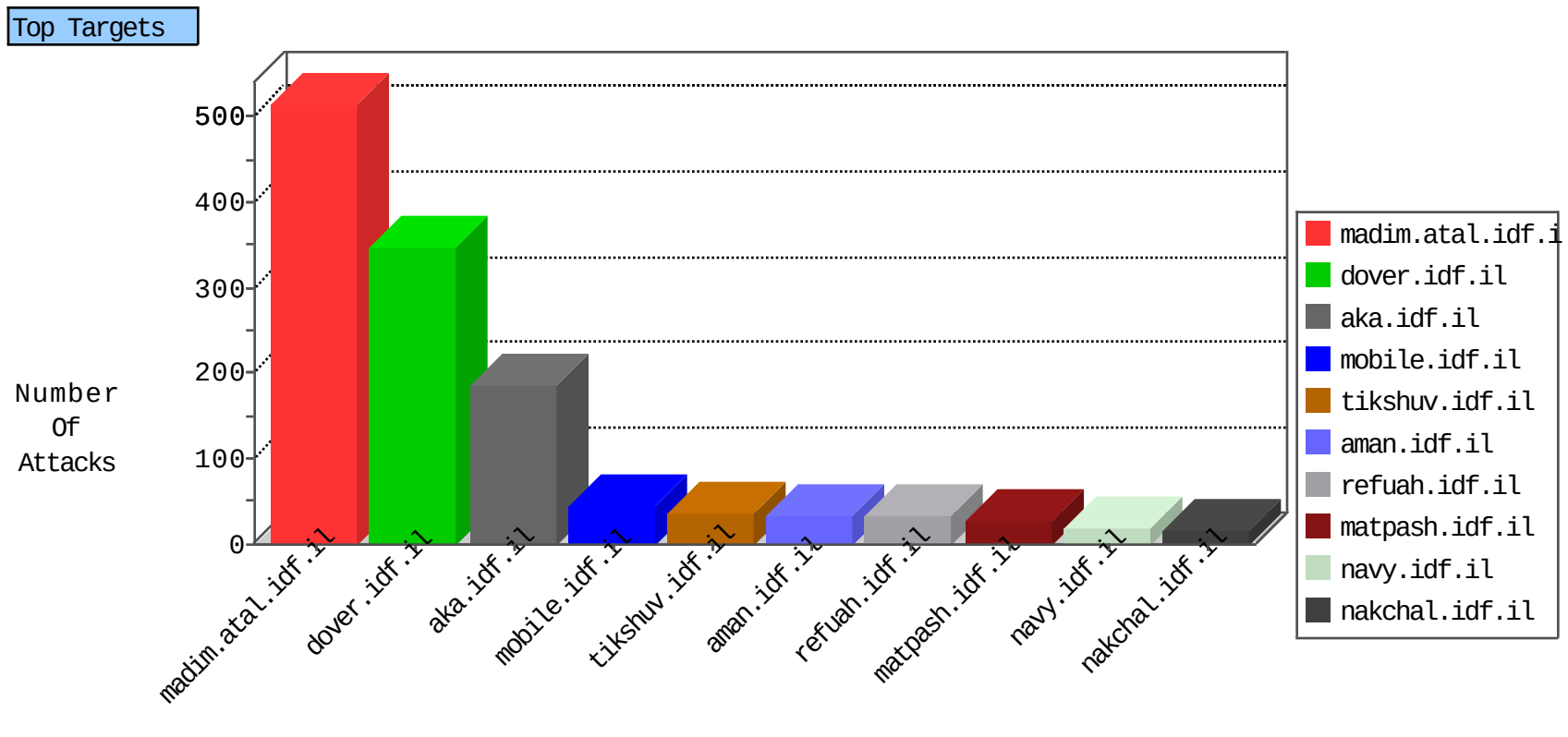
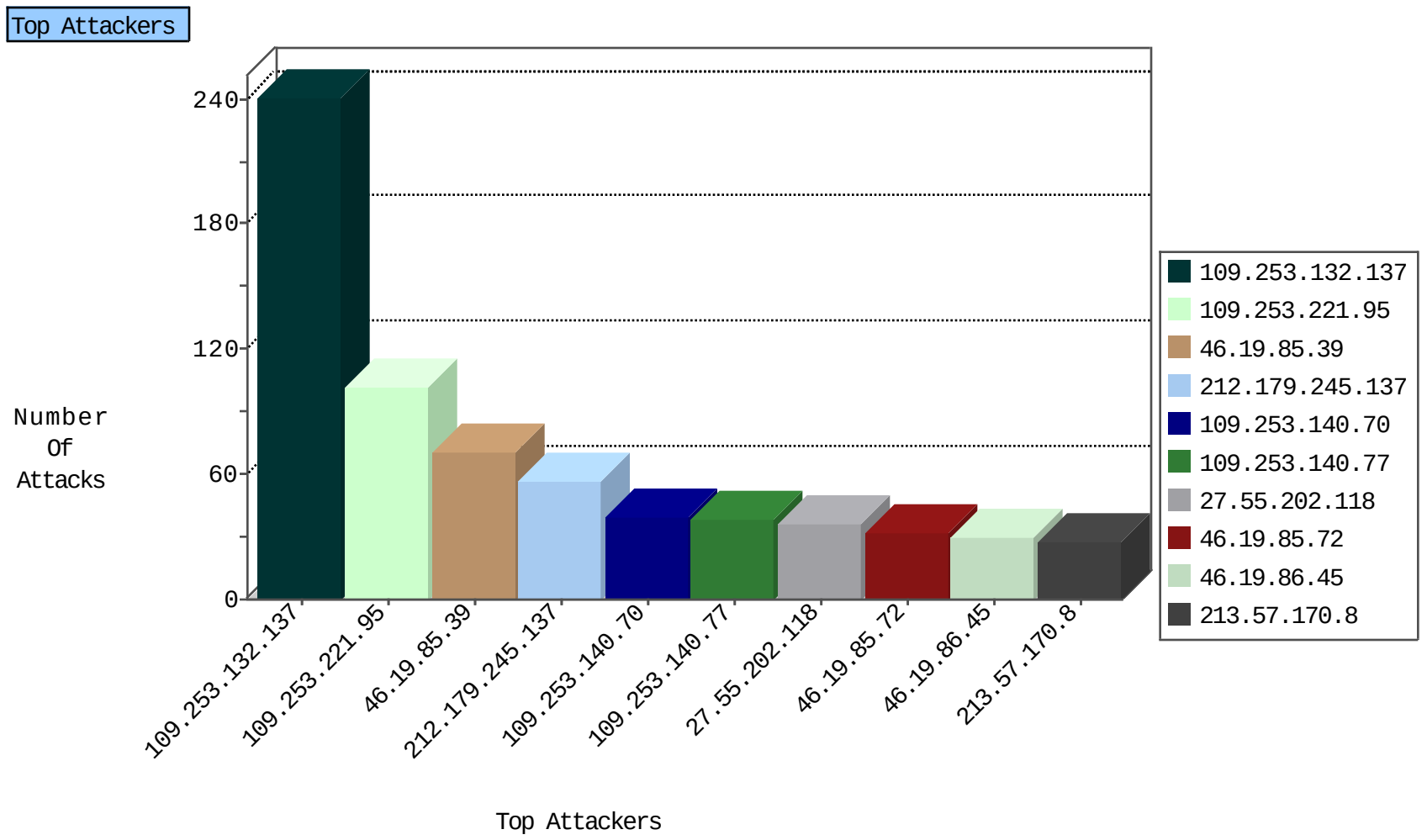
09-21-2016-13:04:02 to 09-21-2016-14:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-21-2016-13:04:02 to 09-21-2016-14:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.25.252	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
46.19.85.133	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
109.67.222.109	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
84.108.27.43	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
52.53.222.9	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
185.24.233.30	Ireland	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
69.30.193.252	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	1
37.26.146.160	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
185.89.217.230	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
45.35.64.142	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
173.208.150.114	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
185.94.111.1	Russian Federation	147.237.76.30	himush.idf.il	Black List	drop	1
80.246.135.51	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
173.208.150.118	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
69.30.193.251	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1
204.12.220.82	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1

09-21-2016-13:04:02 to 09-21-2016-14:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-21-2016-13:04:02 to 09-21-2016-14:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.131	147.237.77.176	Israel	matpash.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	5
84.108.12.255	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
206.246.150.226	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
77.125.12.26	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.129.15	147.237.76.199	United Kingdom	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
141.226.162.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.144.62.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
118.103.126.194	147.237.76.38	Japan	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.211.238	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.226.43.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.163.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.71.44.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.32.167	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
211.149.240.243	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.2.209	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
200.241.137.4	147.237.8.24	Brazil	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
141.226.218.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
118.103.126.194	147.237.77.121	Japan	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.245.103	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.196.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.151.45.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.189.19	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.137.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.235.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
211.149.246.60	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1

09-21-2016-13:04:02 to 09-21-2016-14:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.245.137	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	57
27.55.202.118	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
185.114.254.52	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.86.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
185.114.254.55	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.86.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
109.253.130.126	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
46.19.85.72	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.85.72	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
185.114.254.51	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
185.114.254.54	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
185.137.19.158		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.53.137.103	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
213.57.170.8	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
62.0.221.1	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	8
185.114.254.53	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
213.57.170.8	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.92	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.121.13.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
100.92.136.11		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.25.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.25.252	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.131	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.219.198.6	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.53.18.255	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
62.0.247.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
2.53.18.255	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.2	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
77.126.240.205	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
185.114.254.50	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.176.52.210	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
84.108.27.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.108.27.43	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.131	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Urgent Data Enforcement	TCP segment with urgent pointer (no data). Urgent data indication was stripped. Please refer to sk36869.	drop	4
46.19.86.240	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.92	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
77.124.11.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.101	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.89.217.232	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
213.57.170.8	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.26.148.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.132.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	235
109.253.221.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	102
46.19.85.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	71
109.253.140.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
109.253.140.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	38
46.19.86.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.199.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
81.218.70.243	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 81.218.70.243	Block	5
77.139.204.68	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	3
2.53.8.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
132.74.209.127	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/580-he/patzar.aspx	Block	2
2.53.26.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
85.250.155.171	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	2
212.179.42.225	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	2
37.26.148.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
111.93.113.149	India	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	2
85.250.155.171	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 85.250.155.171	Block	1
68.180.231.43	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.tech.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
212.179.42.225	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.179.42.225	Block	1
41.233.44.63	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.i	Illegal Byte Code Character in URL	Block	1
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/3/	Block	1
192.118.78.57	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/rules.abe	Block	1
89.139.189.19	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/en	Block	1
77.124.23.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
212.179.42.225	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19064-he/	Block	1
46.19.85.36	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl55 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.i	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
198.20.87.98	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/robots.txt	Block	1
66.249.65.160	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1235-he/atal.aspx	Block	1
147.236.238.161	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.i	NULL Character in URL	Block	1
81.218.70.243	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/images/shared/mailthis.gif	Block	1
212.25.85.54	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	1
66.249.66.75	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/iturim/asp/displayallsoldiers.asp	Block	1
2.53.45.94	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.i	Distributed Abnormally Long Request	Block	1
109.253.132.137	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtFirstName in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	1
79.180.212.40	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
46.19.85.217	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout2.css	Block	1
68.180.228.238	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.i	Distributed Unknown HTTP Request Method	Block	1
109.253.134.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized HTTP Method	Block	1
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	1
46.19.86.16	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1

09-21-2016-13:04:02 to 09-21-2016-14:04:02