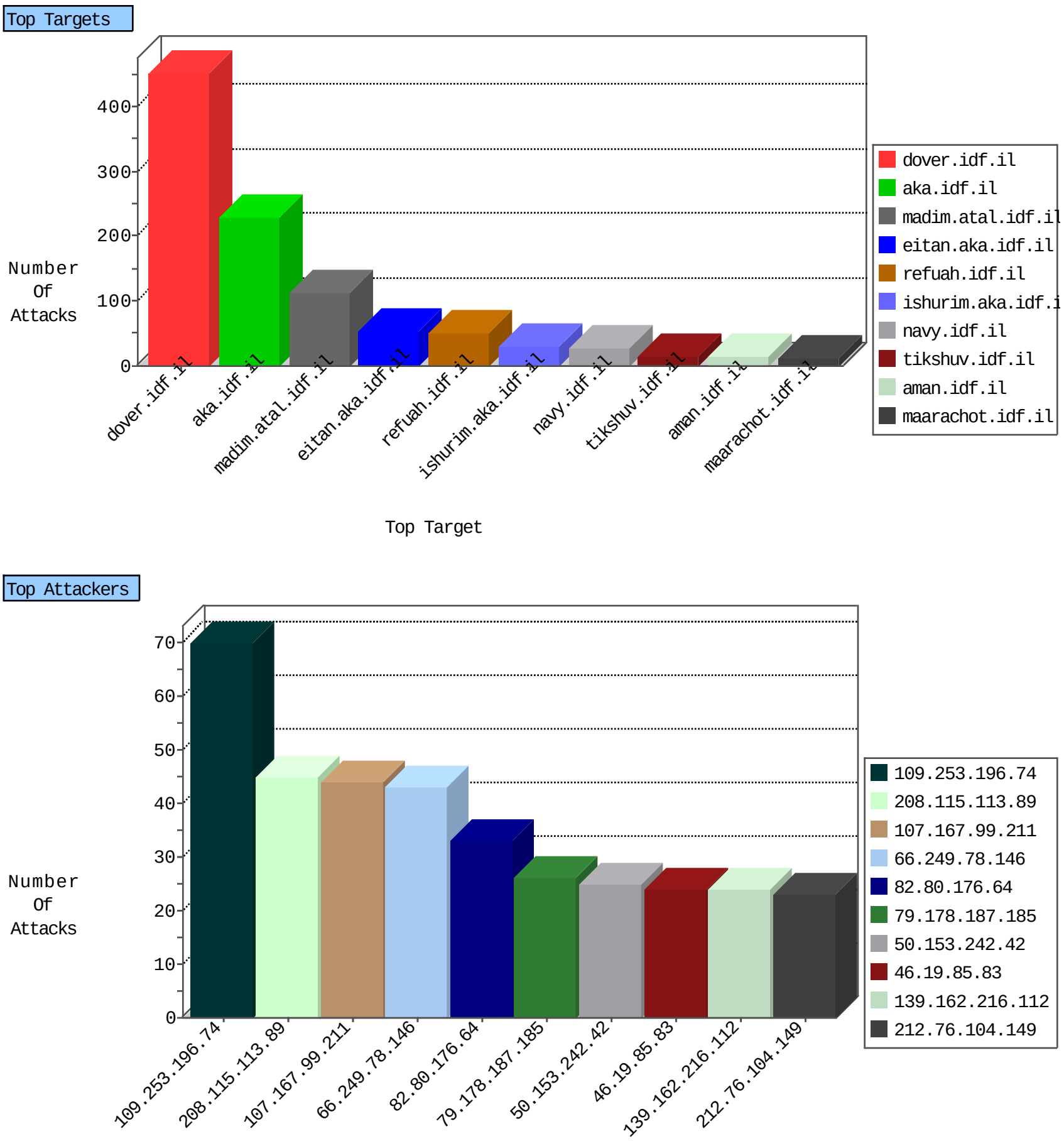
04-26-2016-09:04:08 to 04-26-2016-10:04:08

IDF Under Attack Daily Report



04-26-2016-09:04:08 to 04-26-2016-10:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.97	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	120
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	2
94.102.52.10	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
176.31.60.249	France	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
31.148.219.200	Netherlands	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
94.102.52.10	Netherlands	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1

04-26-2016-09:04:08 to 04-26-2016-10:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
74.84.136.105	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
216.201.148.210	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3

04-26-2016-09:04:08 to 04-26-2016-10:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
74.84.136.105	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
89.248.167.131	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
62.0.41.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
13.92.122.143	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
195.154.54.169	147.237.76.176	France	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
112.217.150.112	147.237.76.198	Korea, Republic of	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.122.143	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
89.248.172.140	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.131	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1

04-26-2016-09:04:08 to 04-26-2016-10:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
107.167.99.211	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	44
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
82.80.176.64	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
79.178.187.185	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
185.104.156.142	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
207.241.231.201	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
24.5.107.9	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
37.26.148.253	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
50.153.242.42	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
82.81.66.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
37.26.148.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
216.177.129.77	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
198.58.103.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
81.218.126.226	Israel	147.237.0.35	akaws.idf.il	drop		drop	11
91.221.58.21	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.55.56.152	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
52.90.38.136	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.65.25.79	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
82.69.124.94	United Kingdom	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
79.176.30.78	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.176.30.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
2.53.128.209	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
87.71.113.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.65.55.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.0.14.218	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.83	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
100.38.228.191	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.83	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
50.153.242.42	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.71.113.85	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
207.46.13.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.64.163.239	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
66.249.81.218	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

04-26-2016-09:04:08 to 04-26-2016-10:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.196.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
212.76.104.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
46.19.85.122	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 46.19.85.122	Block	11
46.19.86.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.146.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.10.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.13.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.191.76	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 81.218.191.76	Block	2
50.153.242.42	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/mobile	Block	2
81.218.191.76	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/- + encodeuri	Block	1
202.180.34.186	Japan	147.237.77.216	dover.idf.il	Illegal HTTP Version proxy error(Cannot Connect)	Block	1
87.70.72.24	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 87.70.72.24	Block	1
79.181.10.20	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
62.128.35.2	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/general/mobile	Block	1
213.57.185.247	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
17.142.157.17	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
82.80.176.64	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
202.180.34.186	Japan	147.237.77.216	dover.idf.il	Malformed URL 560	Block	1
46.19.86.101	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
2.53.3.179	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
89.139.50.66	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl51 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
80.246.130.39	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
65.55.210.170	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
220.255.148.8	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
82.81.82.30	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/homepage/mobile	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
202.180.34.186	Japan	147.237.77.216	dover.idf.il	Unknown HTTP Request Method HTTP/1.1 in URL	Block	1
50.153.242.42	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/pratim/pirteyerua/	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-8847-he/atal.aspx	Block	1
80.246.130.214	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.67	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter PageNum in www.eitan.aka.idf.il/938-en/eitan.aspx	None	1
199.30.24.182	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.122	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/homepage/mobile	Block	1
85.65.26.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.178.6.50	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.32	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
50.153.242.42	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/894-he/eitan.aspx	None	1
2.53.154.16	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/3250.jpg	Block	1
202.180.34.186	Japan	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
87.70.72.24	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
17.142.155.148	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	1

04-26-2016-09:04:08 to 04-26-2016-10:04:08