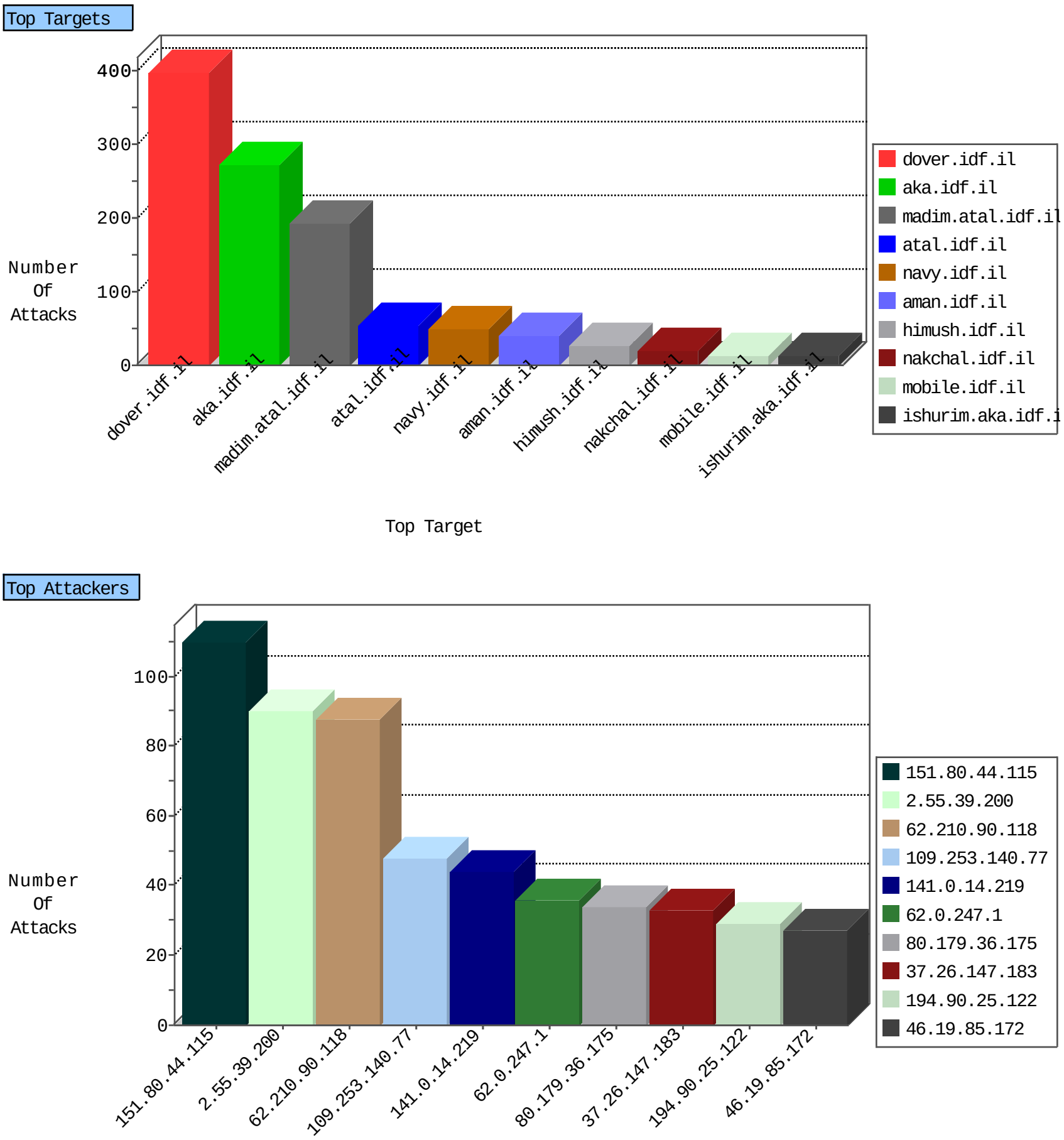
09-21-2016-16:04:02 to 09-21-2016-17:04:02

IDF Under Attack Daily Report



09-21-2016-16:04:02 to 09-21-2016-17:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.0.14.219	Europe	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
141.0.14.219	Europe	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	1
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.76.31	nakchal.idf.il	Black List	drop	1
106.186.113.132	Japan	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	1

09-21-2016-16:04:02 to 09-21-2016-17:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.44.115	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	110
62.210.90.118	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	77
62.210.90.118	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	9
62.210.90.118	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-21-2016-16:04:02 to 09-21-2016-17:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.102.211.105	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	7
46.19.86.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
98.207.0.127	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
41.160.222.18	147.237.8.46	South Africa	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.56.151	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.168.172.139	147.237.76.38	Israel	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.151	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.172.97.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.17.167	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.86.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
211.149.244.79	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.67	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	1
176.13.247.157	147.237.76.30	Israel	himush.idf.il	ET SCAN NMAP -sA (2)	1
46.183.223.228	147.237.76.39	Latvia	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
125.91.109.216	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.19.86.208	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.29.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.56.151	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.26.149.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.56.151	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.168.172.139	147.237.72.156	Israel	aman.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.151	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
5.102.207.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.153.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.18.170	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.24.207.112	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.183.223.228	147.237.77.121	Latvia	e.navy.idf.il	ET SCAN Potential SSH Scan	1
125.213.243.10	147.237.72.217	Thailand	e.idf.il	ET SCAN NMAP -sS window 1024	1
46.121.67.195	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.158.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-21-2016-16:04:02 to 09-21-2016-17:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.0.247.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	36
80.179.36.175	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
141.0.14.219	Europe	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	30
107.167.98.113	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	23
79.178.129.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
79.176.31.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
2.53.6.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
185.32.179.81	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
194.90.25.122	Israel	147.237.76.201	e.atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
141.0.14.219	Europe	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
50.138.15.23	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
50.138.15.23	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
176.13.247.157	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
37.26.147.183	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
37.26.147.183	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
37.26.147.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
79.179.125.202	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
2.53.23.150	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	7
194.90.25.122	Israel	147.237.76.202	e.halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.86.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.143.94	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.53.23.150	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.120.144.213	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
37.26.147.183	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.85.220	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.249.66.247	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN-ACK was acknowledged. Stripping all packet data.	drop	6
37.26.148.216	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
2.53.23.150	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
79.180.163.147	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	5
37.26.148.216	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
212.143.142.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
113.210.201.8	Malaysia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
80.246.138.176	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
176.13.247.157	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
194.90.25.122	Israel	147.237.77.212	e.dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
109.253.143.94	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.55.185.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.134.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.110.84.5	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
5.29.66.121	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.250.121.187	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.86.53	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.53	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
194.242.171.24	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
109.64.41.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.90	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

09-21-2016-16:04:02 to 09-21-2016-17:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.39.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
109.253.140.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
46.19.85.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
119.128.120.163	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 119.128.120.163	Block	12
77.139.139.243	France	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	12
2.55.180.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.86.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
119.128.120.163	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	4
2.55.10.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.197.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.5.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	2
79.180.35.250	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
128.139.12.142	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
31.154.33.190	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
212.235.79.47	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/tizmoret/faq/default.asp	None	2
119.128.120.163	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
66.102.9.26	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
191.96.143.12	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/blog/wp-login.php	Block	1
46.19.86.169	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
77.138.28.251	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
46.120.95.14	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/titlecap.png	Block	1
80.179.36.175	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.134	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
194.242.171.24	France	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.169	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version like Gecko) Version/9.0 Mobile/13G35 Safari/601.1	Block	1
77.138.237.250	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
46.120.144.213	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
80.179.36.175	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.66.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
46.19.86.169	Israel	147.237.77.216	dover.idf.il	Malformed URL (khtml,	Block	1
46.121.141.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.8.6	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.65.98.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.76.113	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/general.aspx	Block	1
46.19.86.169	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method AppleWebKit/601.1.46 in URL (khtml,	Block	1
77.139.139.243	France	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/booklets.aspx	Block	1
191.96.143.12	United States	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	1
89.237.67.27	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
71.6.165.200	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/robots.txt	Block	1

09-21-2016-16:04:02 to 09-21-2016-17:04:02