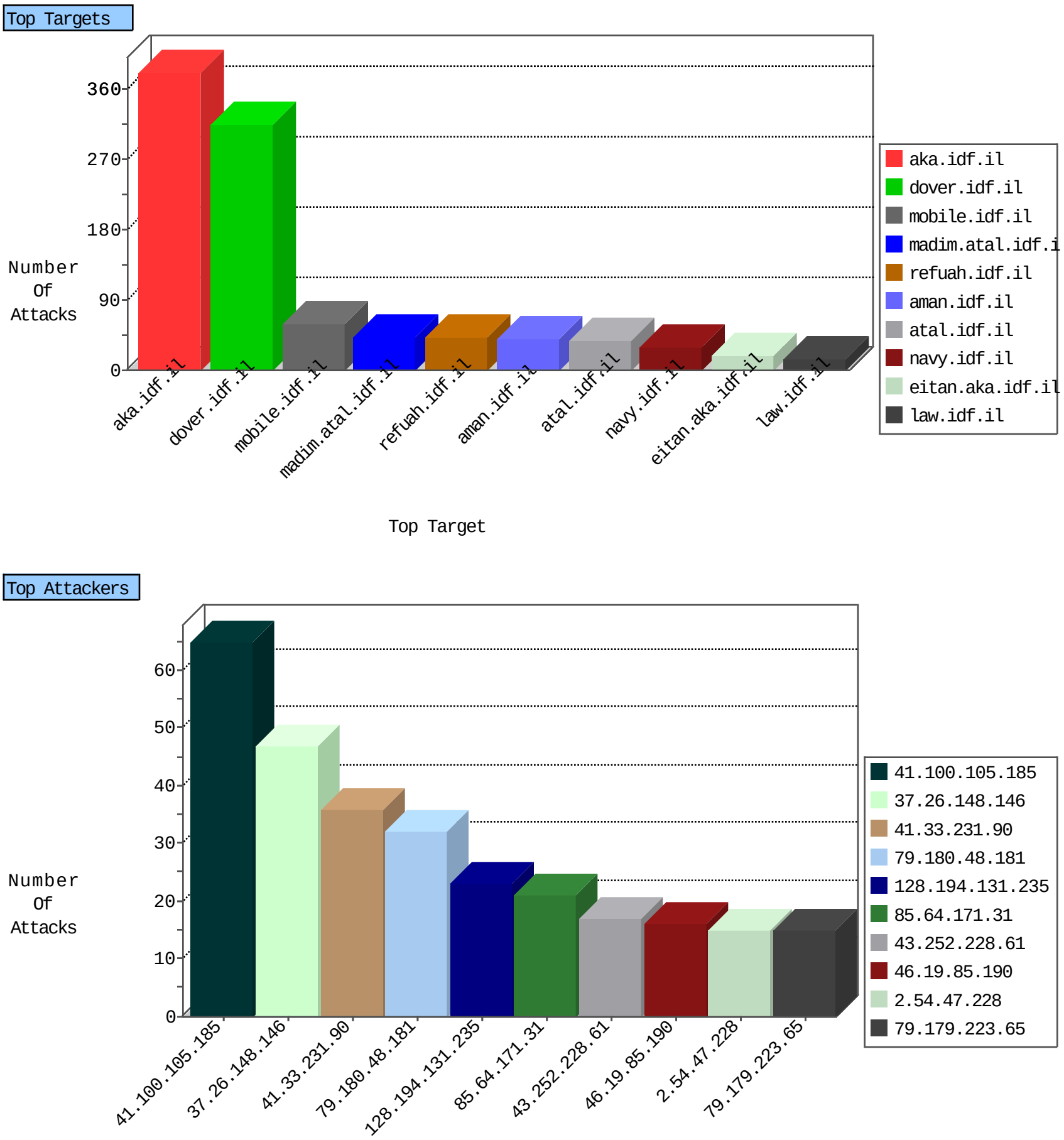
02-09-2016-18:04:05 to 02-09-2016-19:04:05

IDF Under Attack
Daily Report



02-09-2016-18:04:05 to 02-09-2016-19:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.79.127	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2906
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
60.191.74.83	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
128.194.131.235	United States	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
142.54.160.213	United States	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
74.91.28.59	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
212.193.249.95	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
109.67.127.155	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

02-09-2016-18:04:05 to 02-09-2016-19:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
184.173.233.226	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
188.165.15.85	France	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
111.69.150.143	New Zealand	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

02-09-2016-18:04:05 to 02-09-2016-19:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
184.173.233.226	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
43.252.228.61	147.237.76.42	Japan	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.81.204	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.79.10	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.79.127	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
43.252.228.61	147.237.77.212	Japan	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
85.64.194.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
43.252.228.61	147.237.77.178	Japan	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.228.49.170	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
43.252.228.61	147.237.76.196	Japan	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.164.254.228	147.237.76.176	Russian Federation	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
43.252.228.61	147.237.72.217	Japan	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.252.228.61	147.237.72.14	Japan	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
46.19.86.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
43.252.228.61	147.237.0.15	Japan	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
149.88.253.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
43.252.228.61	147.237.77.243	Japan	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.52.186.213	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
115.236.75.201	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
43.252.228.61	147.237.77.227	Japan	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
1.54.210.107	147.237.8.24	Vietnam	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
93.173.231.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
43.252.228.61	147.237.77.179	Japan	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.228.230.32	147.237.72.166	Bulgaria	aka.idf.il	portscan: TCP Distributed Portscan	1
43.252.228.61	147.237.77.61	Japan	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.181.10.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
43.252.228.61	147.237.76.86	Japan	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
77.126.24.228	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
43.252.228.61	147.237.76.38	Japan	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.252.228.61	147.237.72.166	Japan	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
195.159.185.121	147.237.76.38	Norway	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
46.121.142.233	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
43.252.228.61	147.237.0.19	Japan	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.86.82	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.172.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
115.236.75.201	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
43.252.228.61	147.237.77.234	Japan	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
1.54.210.107	147.237.8.24	Vietnam	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
109.186.2.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-09-2016-18:04:05 to 02-09-2016-19:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.100.105.185	Algeria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	65
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
79.180.48.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
37.26.148.146	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
37.26.148.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
85.64.171.31	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
31.168.240.21	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.148.146	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
79.179.223.65	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
46.19.86.241	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
128.194.131.235	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
188.120.148.156	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.66	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
80.246.137.176	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.86.177	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.156.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.90.178.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.120.148.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
81.218.204.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.249.213	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.61	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.75	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.253.202.108	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.225	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.252	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.194.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.2.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.205.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.130	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
159.220.75.7	United Kingdom	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
37.26.148.212	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.179.23.200	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.233.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.48.181	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
216.70.89.222	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.102.254.65	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
188.120.148.160	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.111.50.184	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
109.65.193.173	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
94.230.86.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.17.0	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
149.50.85.16	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.210.187.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.3.147.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
128.194.131.235	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
198.101.157.45	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

02-09-2016-18:04:05 to 02-09-2016-19:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
128.194.131.235	United States	147.237.72.166	aka.idf.il	Distributed NULL Character in Method	Block	6
176.13.12.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.182	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
109.253.202.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
158.69.2.11	United States	147.237.77.74	law.idf.il	Suspicious Response Code	Block	3
46.19.85.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.168.100.81	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	3
46.19.86.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.202.108	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
213.57.238.127	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
46.19.85.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.65.245.175	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$117 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
176.13.3.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.182	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.86.182	Block	2
132.70.66.13	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	2
50.24.196.116	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
46.19.85.196	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
8.37.71.56	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 8.37.71.56	Block	1
85.64.171.31	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
74.91.28.59	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to www.1916wh.com/	Block	1
132.71.70.127	Israel	147.237.77.176	matpash.idf.il	Parameter Type Violation searchText in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
85.250.20.216	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$88 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
80.246.136.130	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	1
213.21.36.105	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Method	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
46.19.85.196	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method n-US;q=0.6,en;q=0.4 in URL	Block	1
8.37.71.56	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1809-he/dover.aspx&usg=alkjrhjjqmsfjuzc6gaaafcbha9ugc7tsa	Block	1
77.125.140.97	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
46.19.86.242	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$LoginControl$captcha$captchaText in aka.idf.il/main/giyus/default.aspx	None	1
94.230.86.177	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
80.246.137.176	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
213.21.36.105	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Byte Code Character in Method from 213.21.36.105	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
46.19.86.1	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
128.194.131.235	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
85.250.20.216	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$42 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
79.179.223.65	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
217.132.83.114	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$35 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.117.127.77	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$35 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
165.91.4.52	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
109.65.193.173	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
2.54.21.209	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.94.72.227	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
213.21.36.105	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple NULL Character in Method from 213.21.36.105	Block	1
66.249.65.18	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/general/general.aspx	Block	1
37.142.68.58	Israel	147.237.72.166	aka.idf.il	Unknown Parameter x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
85.250.20.216	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$67 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
79.180.56.172	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1

02-09-2016-18:04:05 to 02-09-2016-19:04:05