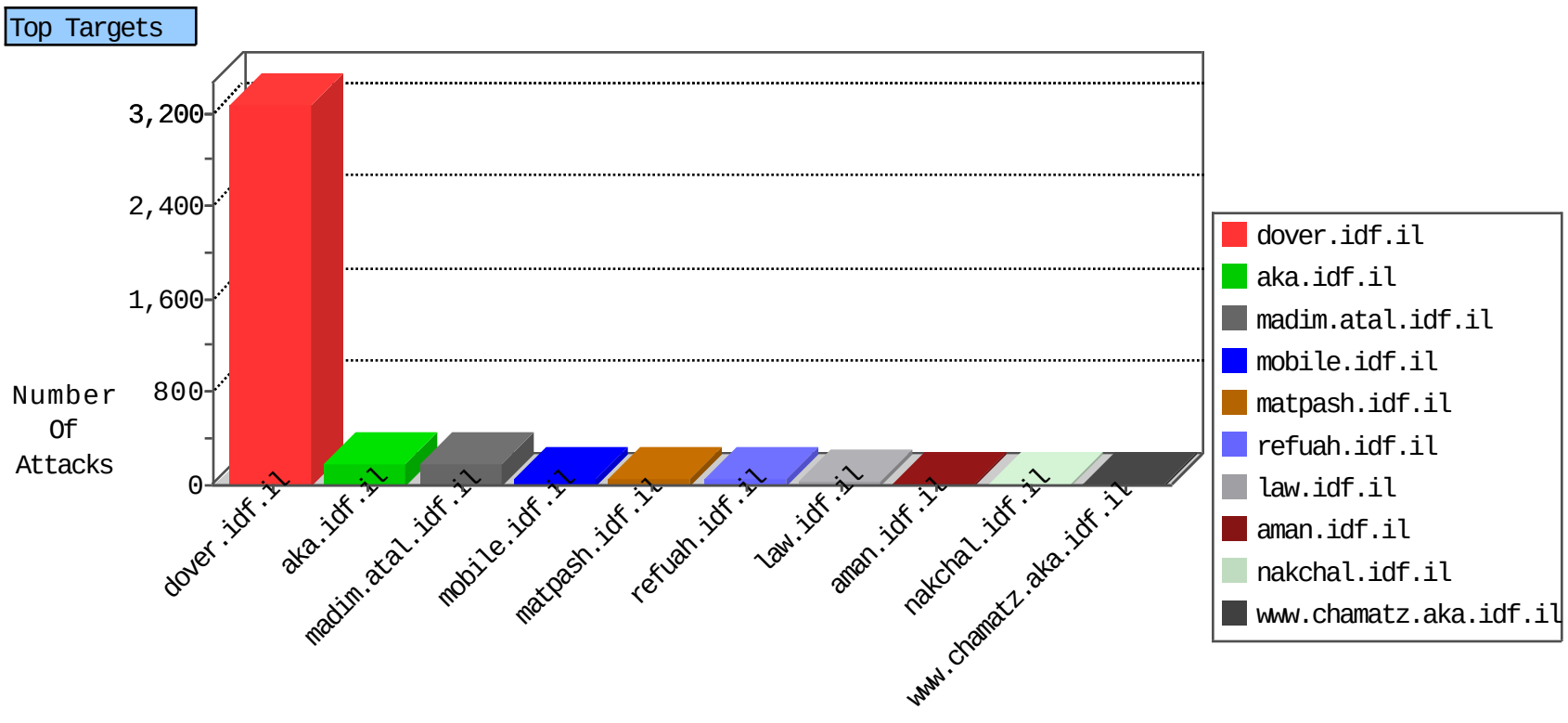
02-17-2016-21:04:05 to 02-17-2016-22:04:05

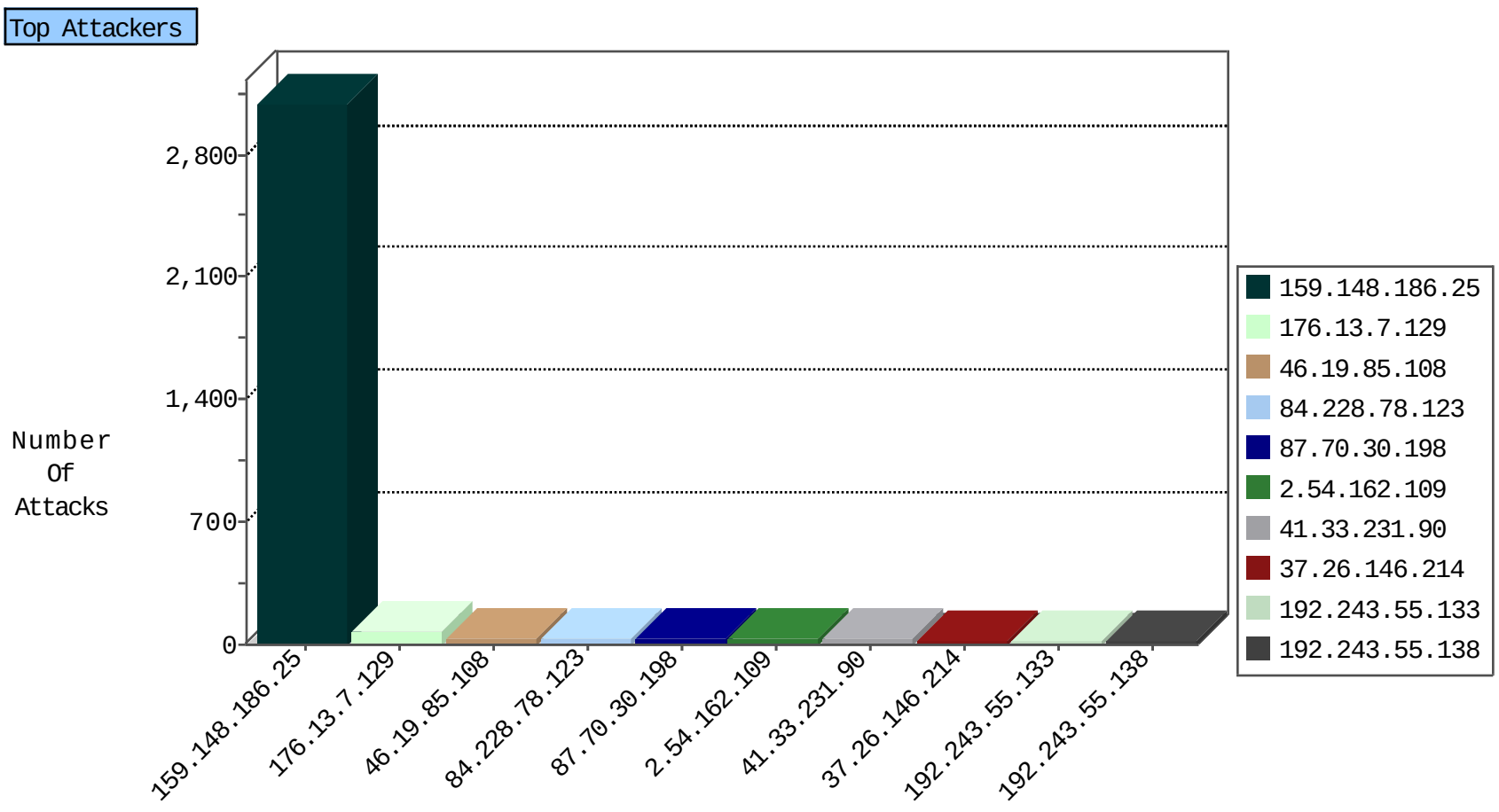
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-17-2016-21:04:05 to 02-17-2016-22:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
159.148.186.25	Latvia	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3731
159.148.186.25	Latvia	147.237.77.216	dover.idf.il	HTTP-MISC-Slow-HTTP-Test-DoS	source-reset	2549
109.67.10.142	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
159.148.186.25	Latvia	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	4
185.130.5.224		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
64.110.129.208		147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
69.30.218.62	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1

02-17-2016-21:04:05 to 02-17-2016-22:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.211	Israel	147.237.77.216	dover.idf.i	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

02-17-2016-21:04:05 to 02-17-2016-22:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
148.163.122.135	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
148.163.122.135	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
87.71.23.106	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
63.221.141.195	147.237.76.201	Hong Kong	e.atal.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
63.221.141.195	147.237.76.176	Hong Kong	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
190.216.146.151	147.237.77.216	Chile	dover.idf.il	ET SCAN Potential SSH Scan	1
63.221.141.195	147.237.0.16	Hong Kong	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
190.216.146.151	147.237.0.16	Chile	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
188.64.169.106	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.60.252.84	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
148.163.122.135	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
93.172.189.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.204.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
63.221.141.195	147.237.76.199	Hong Kong	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
63.221.141.195	147.237.76.147	Hong Kong	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
190.216.146.151	147.237.0.33	Chile	idf.il	ET SCAN Potential SSH Scan	1
188.64.169.106	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.240	147.237.77.176		matpash.idf.il	ET SCAN NMAP -sS window 1024	1

02-17-2016-21:04:05 to 02-17-2016-22:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
159.148.186.25	Latvia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1991
159.148.186.25	Latvia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	234
84.228.78.123	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
159.148.186.25	Latvia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
46.19.86.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.66.174.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.54.38.196	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.142.68.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
159.148.186.25	Latvia	147.237.77.216	dover.idf.il	SYN Attack		reject	6
37.26.146.214	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.253.216.243	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.160.167.29	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.137.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.126.22.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.137	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.85.140	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
185.24.206.56	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
85.115.52.201	United Kingdom	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
185.24.206.56	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.133	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
85.250.57.174	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.24.206.56	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
68.180.231.40	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
185.32.179.228	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
37.26.146.214	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
185.32.179.228	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
141.0.15.241	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.146.214	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	4
185.32.179.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.64.167.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.36.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
79.177.28.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
217.132.30.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.166.247.138	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.68.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.178	Israel	147.237.77.226	www.chamatz.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
128.242.249.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.95	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.177.127.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.143.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.210.199.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.31.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

02-17-2016-21:04:05 to 02-17-2016-22:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.7.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	78
46.19.85.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
87.70.30.198	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	36
2.54.162.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	35
212.76.122.21	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 212.76.122.21	Block	5
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	4
37.26.149.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.137.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.157.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.159.99	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.142.245.136	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	2
82.166.247.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
42.2.226.195	Hong Kong	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.108.144.234	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/kkkkkkk=40ee37adkkkkkkk_40ee37ad	Block	1
66.249.69.48	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20387-he/dover.aspx	Block	1
109.253.213.237	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$3 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
5.102.221.209	Israel	147.237.77.74	law.idf.il	Parameter Type Violation SearchText in www.law.idf.il/163-6639-he/patzar.aspx	Block	1
85.115.52.201	United Kingdom	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
81.218.251.250	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized HTTP Method	Block	1
212.76.122.21	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.76.122.21	Block	1
157.55.39.23	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
52.30.171.229	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on /	Block	1
109.64.19.7	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
40.77.167.38	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.108.236.54	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	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
46.19.85.204	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
87.68.254.48	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.68.254.48	Block	1
81.218.251.250	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/901-8125-he/	Block	1
212.76.125.186	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.76.125.186	Block	1
157.55.39.94	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.240.192.138	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
40.77.167.43	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/lobby/lobby.aspx	Block	1
84.109.25.76	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$2 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
77.126.24.250	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.85.249	Israel	147.237.77.176	matpash.idf.il	Malformed URL	Block	1
148.251.21.227	Germany	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
87.68.254.48	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	1
212.76.125.186	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/&sa=u&ved=0ahukewimx4tlyp_kahvbexikha_lbhoqfggimaa&usg=afqjcnhcdsh5ryhkeugapxldsq7fowjwnw	Block	1
162.243.175.22	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/25/	Block	1
84.228.78.123	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
77.127.224.171	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.249	Israel	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method pjsw5l45 in URL	Block	1
148.251.21.227	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/×″×?×ª×¨	Block	1
38.81.65.42	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1

02-17-2016-21:04:05 to 02-17-2016-22:04:05