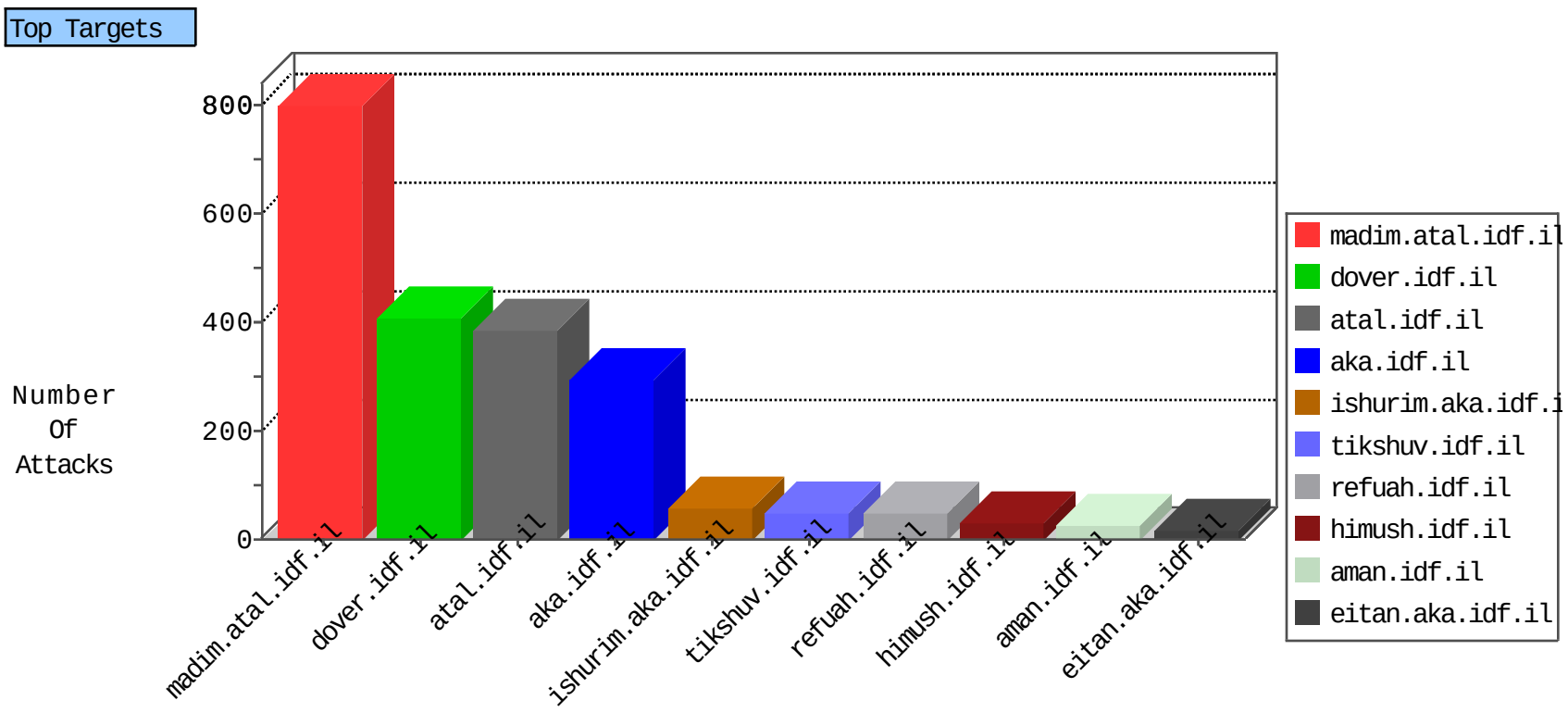
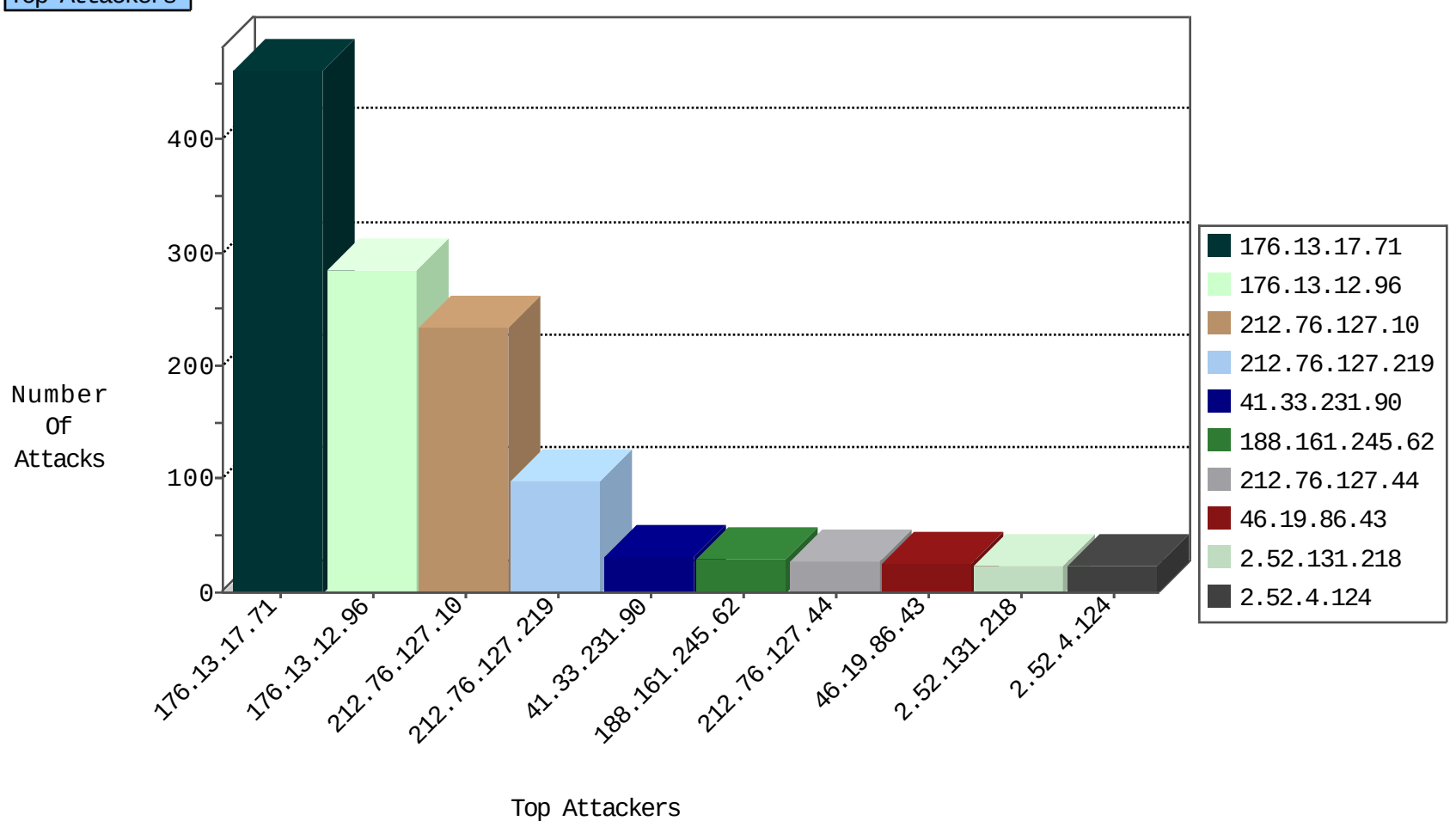
02-16-2016-18:04:04 to 02-16-2016-19:04:04

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-16-2016-18:04:04 to 02-16-2016-19:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.130.5.224		147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
167.114.133.208	Canada	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

02-16-2016-18:04:04 to 02-16-2016-19:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.125.125.76	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
172.86.83.125		147.237.77.233	atal.idf.il	0543: HTTP: php.cgi Access	Block	1
94.102.56.143	Netherlands	147.237.76.86	navy.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

02-16-2016-18:04:04 to 02-16-2016-19:04:04

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
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
94.182.163.74	147.237.76.200	Iran, Islamic Republic of	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
69.197.145.242	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
103.53.52.107	147.237.77.74		law.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
94.182.163.74	147.237.76.197	Iran, Islamic Republic of	e.himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
103.53.52.107	147.237.76.201		e.atal.idf.il	ET SCAN Potential SSH Scan	1
94.182.163.74	147.237.76.30	Iran, Islamic Republic of	himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
103.53.52.107	147.237.76.86		navy.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.103	147.237.72.167		ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
103.53.52.107	147.237.76.42		refuah.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
148.251.21.227	147.237.72.166	Germany	aka.idf.il	portscan: TCP Distributed Portscan	1
103.53.52.107	147.237.76.31		nakchal.idf.il	ET SCAN Potential SSH Scan	1
37.142.68.67	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.214.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.172.198	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
103.53.52.107	147.237.72.166		aka.idf.il	ET SCAN Potential SSH Scan	1
27.221.10.194	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
103.53.52.107	147.237.77.235		sviva.idf.il	ET SCAN Potential SSH Scan	1
84.108.193.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.162.195	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
103.53.52.107	147.237.0.34		tikshuv.idf.il	ET SCAN Potential SSH Scan	1
103.53.52.107	147.237.77.216		dover.idf.il	ET SCAN Potential SSH Scan	1
84.94.80.212	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
103.53.52.107	147.237.0.17		m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
79.176.178.219	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
103.53.52.107	147.237.77.176		matpash.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
94.182.163.74	147.237.76.198	Iran, Islamic Republic of	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
62.90.96.102	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
103.53.52.107	147.237.76.202		e.halag.idf.il	ET SCAN Potential SSH Scan	1
94.182.163.74	147.237.76.44	Iran, Islamic Republic of	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
213.8.204.85	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
103.53.52.107	147.237.76.176		test.ncore.idf.il	ET SCAN Potential SSH Scan	1
94.182.163.74	147.237.0.17	Iran, Islamic Republic of	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.240	147.237.76.147		chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
103.53.52.107	147.237.76.44		e.refuah.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
149.88.171.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
103.53.52.107	147.237.76.34		yohalan.idf.il	ET SCAN Potential SSH Scan	1
93.173.25.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.196.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-16-2016-18:04:04 to 02-16-2016-19:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	228
212.76.127.219	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	99
188.161.245.62	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
212.76.127.44	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	27
2.52.131.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.43	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	23
46.121.120.173	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
77.125.117.217	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
136.173.162.144	Belgium	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.4.124	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
80.246.130.110	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
46.19.86.138	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.9	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
173.201.196.209	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
46.19.85.112	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
79.179.152.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.76.127.10	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
109.65.26.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.112	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.36.25	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.8.40	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.120.126.58		147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.37.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.40.105	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.4	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.179	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.116	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
198.204.249.34	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.161	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.182.53.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.131.93	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.161	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
31.210.186.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.17.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	252
176.13.12.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	142
176.13.12.96	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.12.96	Block	122
176.13.17.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	106
176.13.17.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
176.13.12.96	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.13.12.96	Block	21
85.65.202.14	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
176.13.20.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
80.246.137.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
82.166.116.87	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.166.116.87	Block	9
46.19.85.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
82.166.116.87	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	5
176.13.4.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
172.86.83.125		147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 172.86.83.125	Block	3
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.1.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.202.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
94.102.56.143	Netherlands	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 94.102.56.143	Block	2
91.226.4.171	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'	Block	2
37.142.159.13	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.142.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
94.102.56.143	Netherlands	147.237.76.86	navy.idf.il	PHP Attempt	Block	2
84.108.218.123	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.108.218.123	Block	2
109.160.158.232	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$83 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	2
82.110.109.208	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	2
2.54.136.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
93.172.135.104	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/994-8516-he/himush.aspx#.vsnan78l1bo.facebook	Block	2
109.253.146.92	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
199.30.24.97	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.12.90	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
213.57.160.179	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$90 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
37.46.39.239	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$88 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.186.0.45	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$22 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
82.110.109.210	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.125.117.217	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
176.228.192.9	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
2.54.185.184	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$38 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
94.102.56.143	Netherlands	147.237.76.86	navy.idf.il	Admin Blocking	Block	1
87.68.245.82	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	1
82.166.116.87	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
46.19.85.85	Israel	147.237.0.34	tikshuv.idf.il	Abnormally Long Request request version	Block	1
5.29.249.7	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 5.29.249.7 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
109.67.32.156	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
79.180.98.101	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
207.81.10.239	Canada	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
89.138.176.136	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/	Block	1