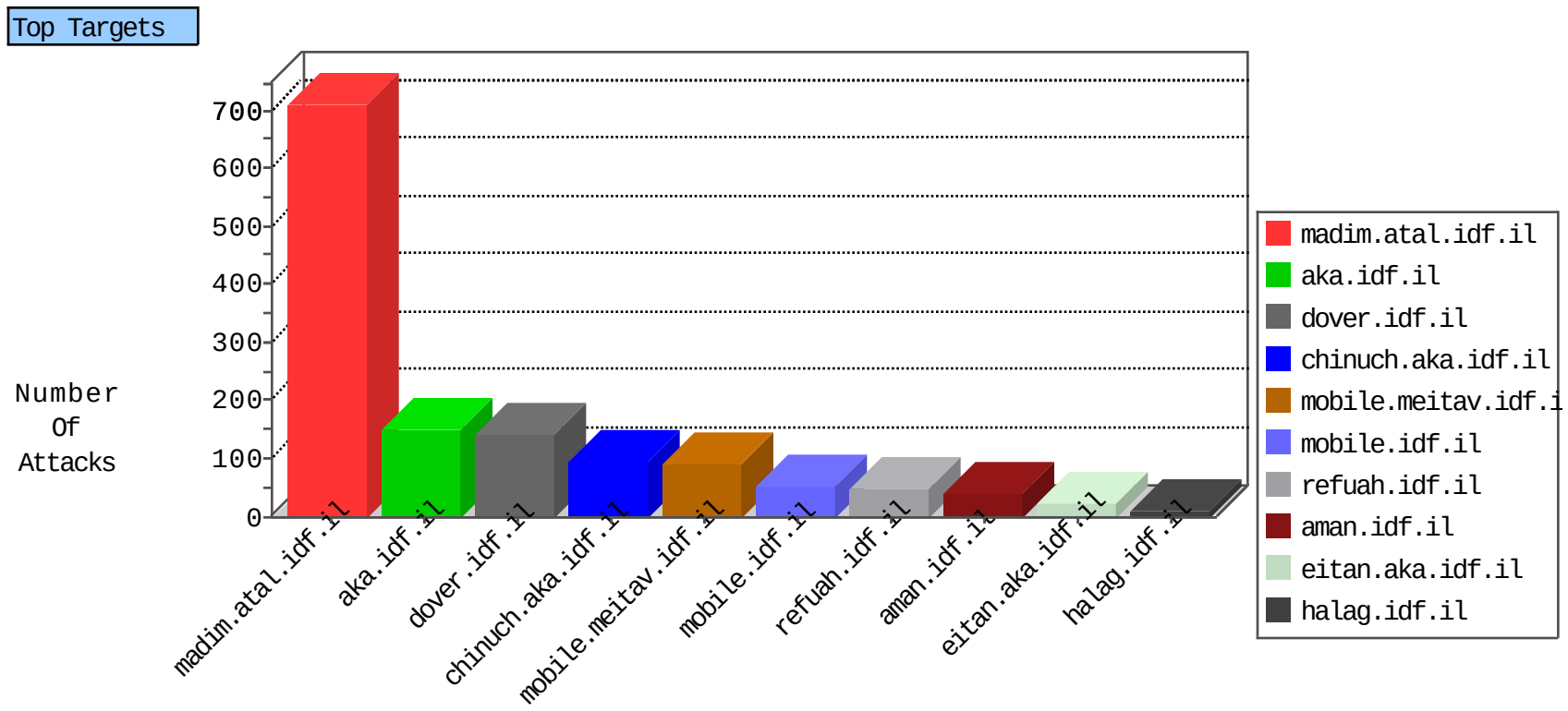
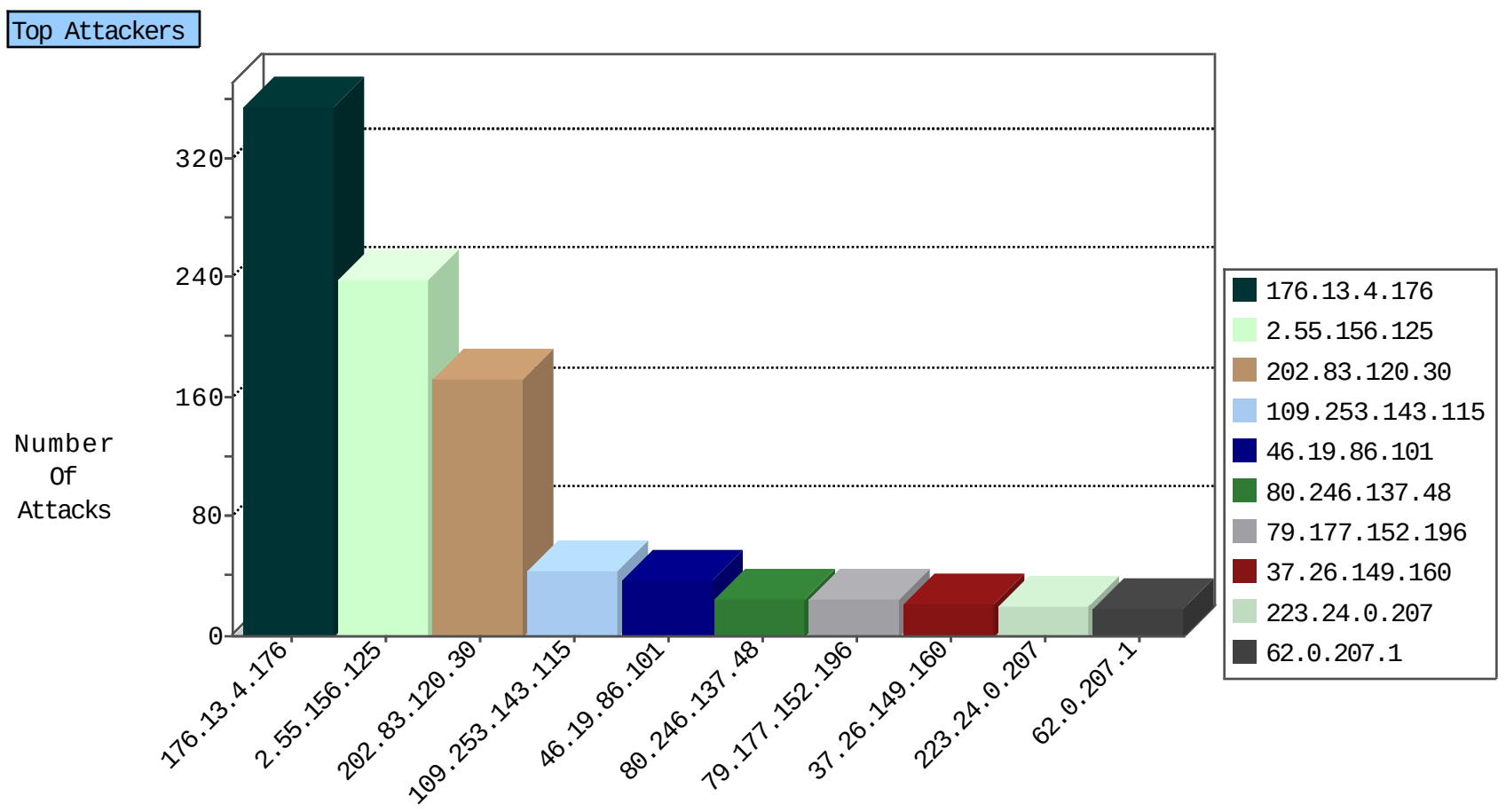
09-25-2016-17:04:00 to 09-25-2016-18:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-25-2016-17:04:00 to 09-25-2016-18:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.76.39	mobile.meitav.idf.il	Black List	drop	2
93.174.94.235	Netherlands	147.237.76.177	ncore.idf.il	Black List	drop	1
63.141.231.198	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
69.64.61.103	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	1
178.239.62.141	Netherlands	147.237.76.30	himush.idf.il	Black List	drop	1
80.72.33.56	Poland	147.237.76.176	test.ncore.idf.il	Black List	drop	1

09-25-2016-17:04:00 to 09-25-2016-18:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.68.101	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-25-2016-17:04:00 to 09-25-2016-18:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
192.115.67.2	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	6
185.159.36.2	147.237.76.197		e.himush.idf.il	ET SCAN Potential SSH Scan	2
185.159.36.2	147.237.76.34		yohalan.idf.il	ET SCAN Potential SSH Scan	2
79.177.221.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.69	147.237.76.42	Europe	refuah.idf.il	ET SCAN NMAP -sA (2)	1
185.159.36.2	147.237.76.148		gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
46.161.40.17	147.237.76.34	Russian Federation	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.66.154	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.237.93	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.215.36.46	147.237.72.167	Kenya	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.60.153.178	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.203.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.204.15.134	147.237.77.216	Russian Federation	dover.idf.il	ET WEB_SERVER PyCurl Suspicious User Agent Inbound	1
87.69.232.91	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.1.39	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.159.36.2	147.237.76.199		e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
79.177.137.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.159.36.2	147.237.76.196		e.sviva.idf.il	ET SCAN Potential SSH Scan	1
46.183.223.228	147.237.76.86	Latvia	navy.idf.il	ET SCAN Potential SSH Scan	1
185.159.36.2	147.237.76.38		e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
46.161.40.17	147.237.0.15	Russian Federation	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.159.36.2	147.237.76.30		himush.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.124	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.68.144.93	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.49.104	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.216.252.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.238.229	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.22.2.142	147.237.72.167	Bulgaria	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.159.36.2	147.237.76.200		eitan.aka.idf.il	ET SCAN Potential SSH Scan	1

09-25-2016-17:04:00 to 09-25-2016-18:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.177.152.196	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
223.24.0.207	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
46.19.86.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	19
62.0.207.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	19
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	18
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
80.246.137.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.86.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	16
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	16
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	14
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	14
79.180.156.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
69.22.185.204	United States	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.248	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
176.13.9.216	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
89.139.187.80	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
185.32.179.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.19.85.248	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.13.248.47	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.140.1	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
80.246.136.224	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
213.57.9.151	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.54	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
69.65.83.151	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
2.55.182.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
213.57.252.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
176.13.228.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.255	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
80.246.130.196	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
212.199.57.199	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.66	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.117.6.206	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
79.180.254.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.84	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
87.69.105.14	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
79.180.254.77	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
109.253.129.22	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
192.116.177.146	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.180.107.221	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

09-25-2016-17:04:00 to 09-25-2016-18:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.4.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	354
2.55.156.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	238
109.253.143.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
37.26.149.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
176.13.20.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
80.246.139.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
185.32.179.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
80.246.137.48	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
85.65.190.124	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	4
109.253.215.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.140.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.182.87.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.115.67.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
37.26.147.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.22.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.137.48	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.248.47	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.138.59.1	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Distributed Unknown HTTP Request Method	Block	1
84.95.208.20	Israel	147.237.72.167	ishurim.aka.idf.i	PHP Attempt	Block	1
79.180.183.24	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/givus	Block	1
46.120.245.200	Israel	147.237.72.167	ishurim.aka.idf.i	SSL Untraceable Connection - Unknown SSL Session	None	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
77.138.107.34	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in Header Name	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
141.226.232.17	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
80.246.137.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.30.230	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in Method ,[[#25]]¢Ma1¨àa¾vØÓæ]²=nU“çôÚí[[#0]]œ'…táÐV2D›Xà[[#3]]—Í™[[#21]]Ì Tb	Block	1
79.183.34.168	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/	Block	1
66.249.76.85	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/3296.jpg	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Distributed Abnormally Long Request	Block	1
207.46.13.31	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
77.139.54.181	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	NULL Character in Method ,[[#25]]¢Ma1¨àa¾vØÓæ]²=nU“çôÚí[[#0]]œ'…táÐV2D›Xà[[#3]]—Í™[[#21]]Ì Tb	Block	1
89.139.187.80	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
80.246.130.196	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/61998	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Distributed Malformed URL	Block	1
2.53.150.209	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
213.151.35.213	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
79.178.245.175	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ גאדיום	Block	1
37.26.149.165	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1

09-25-2016-17:04:00 to 09-25-2016-18:04:00