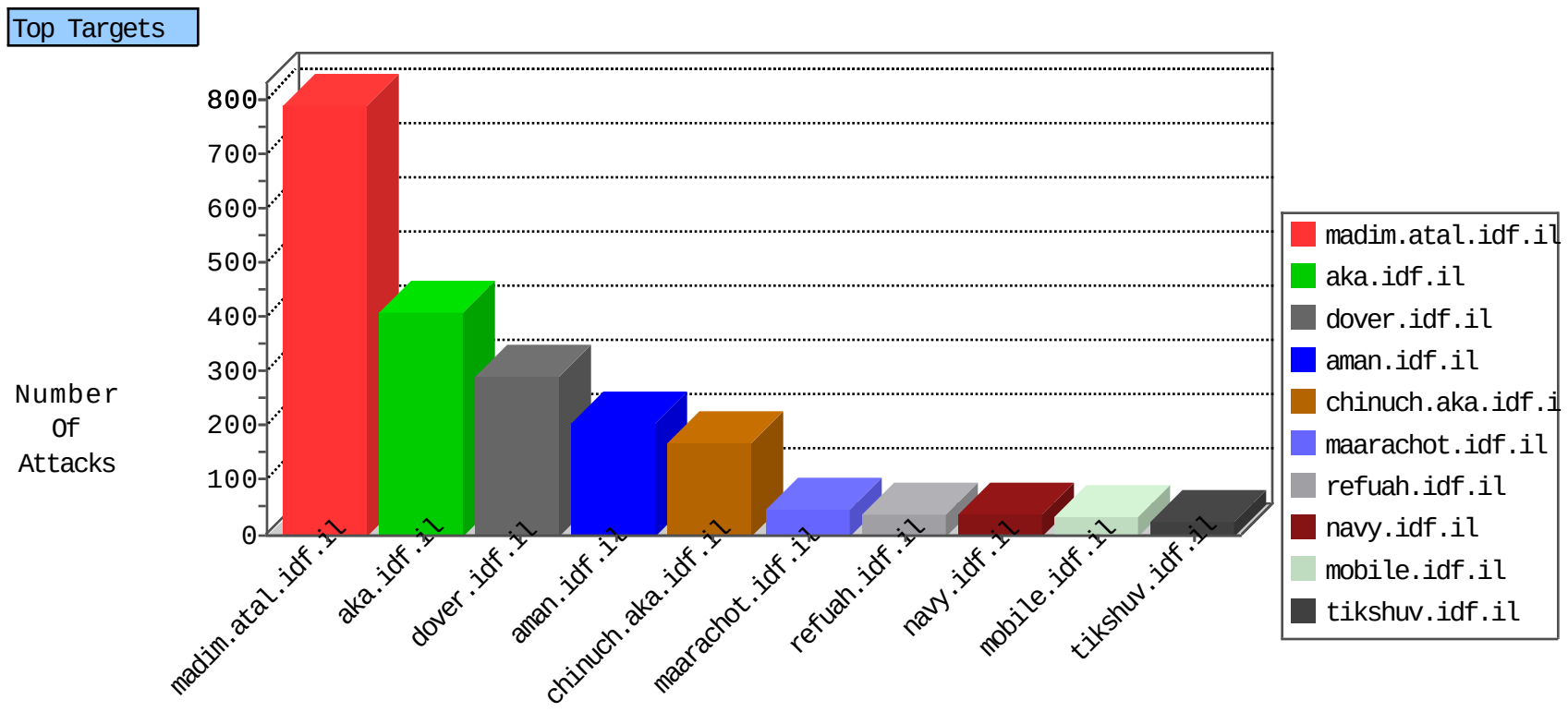
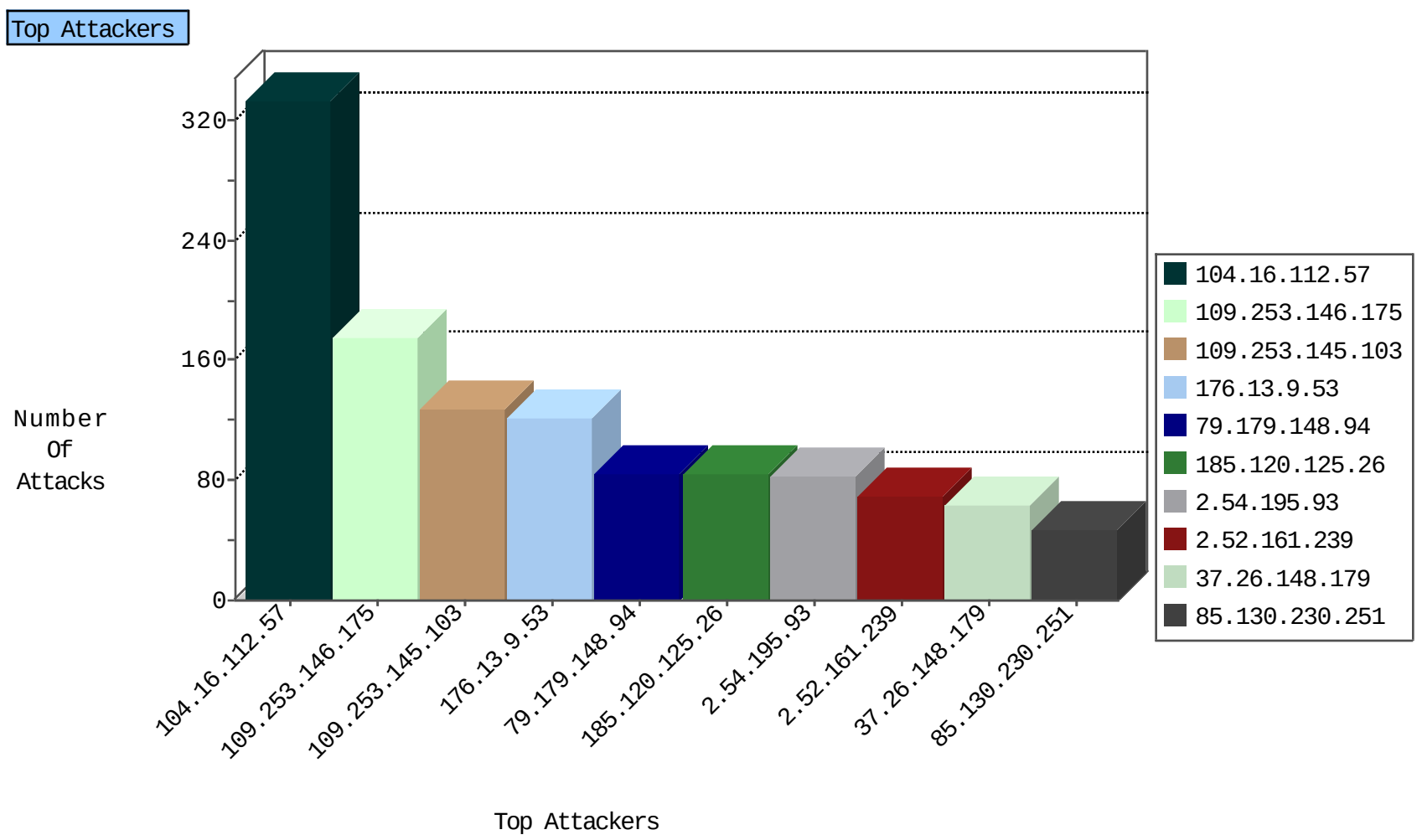
02-07-2016-18:04:01 to 02-07-2016-19:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-07-2016-18:04:01 to 02-07-2016-19:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
101.228.171.103	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
107.191.42.168	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
31.202.128.149	Ukraine	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
142.54.160.211	United States	147.237.77.234	halag.idf.il	block-sp-traf1	drop	1
74.91.28.58	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1
185.130.5.201		147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
31.202.128.149	Ukraine	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
222.190.113.226	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
31.202.128.149	Ukraine	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1

02-07-2016-18:04:01 to 02-07-2016-19:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.98.86.210	Turkey	147.237.77.74	law.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
123.126.68.114	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

02-07-2016-18:04:01 to 02-07-2016-19:04:01

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
66.249.65.224	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sA (2)	2
46.121.103.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.130.169.225	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
37.26.147.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.190.113.226	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
104.130.169.225	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
222.190.113.226	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
5.29.21.36	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.130.169.225	147.237.72.217	United States	e.idf.il	ET SCAN Potential SSH Scan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
98.82.54.39	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
85.98.86.210	147.237.77.74	Turkey	law.idf.il	SERVER-WEBAPP admin.php access	1
146.185.250.2	147.237.8.27	Russian Federation	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
79.178.205.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.68.111.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.162.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.160.147.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.49.111	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.121.65.48	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.130.169.225	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
5.234.220.229	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	portscan: TCP Distributed Portscan	1
222.190.113.226	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
104.130.169.225	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
213.8.204.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.128.144.131	147.237.76.202	Canada	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
212.116.164.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.207.60.30	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.108.76.169	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
146.185.250.2	147.237.8.14	Russian Federation	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
78.193.2.8	147.237.77.176	France	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
123.196.116.66	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
77.125.133.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.159.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-07-2016-18:04:01 to 02-07-2016-19:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
104.16.112.57	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	165
104.16.112.57	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	165
185.120.125.26		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
185.120.125.26		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
2.52.161.239	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
85.130.230.251	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
79.176.56.142	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
85.130.230.251	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
2.54.195.93	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
2.54.195.93	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
85.130.230.251	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	13
2.52.161.239	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
2.52.161.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
5.234.220.229	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
2.52.161.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
5.234.220.229	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
5.22.130.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.161.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
2.54.195.93	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
87.69.211.63	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
5.22.135.180	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.54.40.80	Israel	147.237.77.243	mobile.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	9
46.19.86.118	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
77.125.153.50	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
80.246.139.192	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.85.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
79.179.208.232	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.106.46.38	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.194	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.194	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.32	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.167.91	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.76.127.10	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
37.26.149.190	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
185.120.125.17		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.147.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.230	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.116.147.104	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.178.37.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
37.46.35.113	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
213.151.35.213	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
31.210.188.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.168.2.130	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.116.158.98	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
31.210.188.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

02-07-2016-18:04:01 to 02-07-2016-19:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.146.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	92
79.179.148.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	83
109.253.145.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	83
109.253.146.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	83
176.13.9.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	72
37.26.148.179	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
176.13.9.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	49
109.253.145.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	45
2.54.195.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	40
176.13.3.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
2.54.135.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	31
46.19.85.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
80.246.137.121	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
46.19.86.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/watch	Block	9
2.54.183.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
79.178.166.144	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	5
85.98.86.210	Turkey	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 85.98.86.210	Block	5
85.98.86.210	Turkey	147.237.77.74	law.idf.il	PHP Attempt	Block	4
149.50.80.21	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.50.80.21	Block	3
85.98.86.210	Turkey	147.237.77.74	law.idf.il	Multiple Admin Blocking from 85.98.86.210	Block	3
37.26.148.179	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	3
2.54.40.80	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.211.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
185.24.76.131	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
46.120.106.197	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$14 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
46.19.86.118	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.1.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
185.27.106.70	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
146.185.234.48	Russian Federation	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 146.185.234.48	Block	2
81.218.207.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
31.168.210.53	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
37.26.146.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.230	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.65.41.206	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	1
85.98.86.210	Turkey	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
46.120.106.197	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$102 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
194.90.88.105	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
176.13.1.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
84.109.189.139	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.178.15.212	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$1 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.121.65.48	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
100.2.169.4	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.98.86.210	Turkey	147.237.77.74	law.idf.il	Admin Blocking	Block	1
79.183.153.60	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
37.26.148.130	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
149.50.80.21	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gitus	Block	1
77.125.153.50	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.52.9.126	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/926-he/refuah.aspx	Block	1

02-07-2016-18:04:01 to 02-07-2016-19:04:01