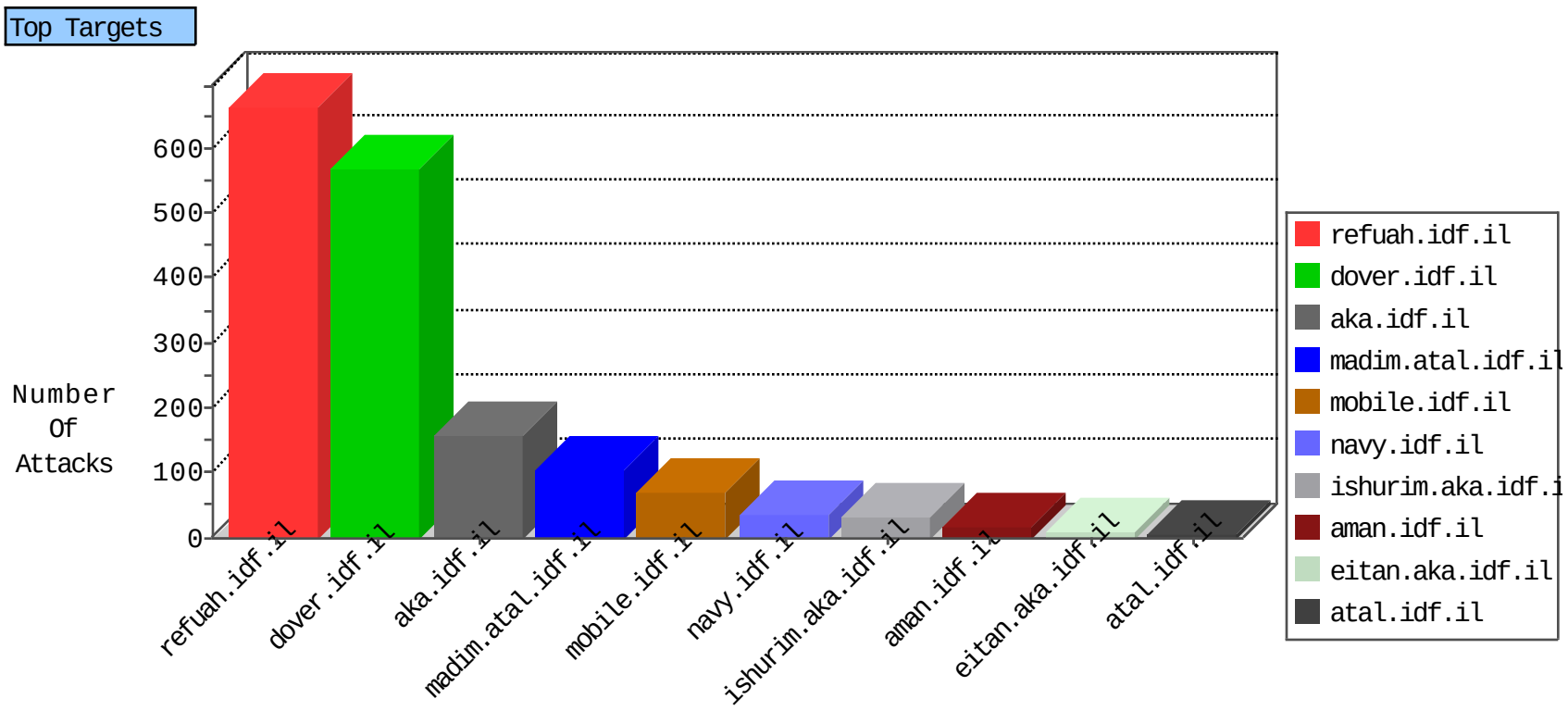
09-14-2016-08:04:05 to 09-14-2016-09:04:05

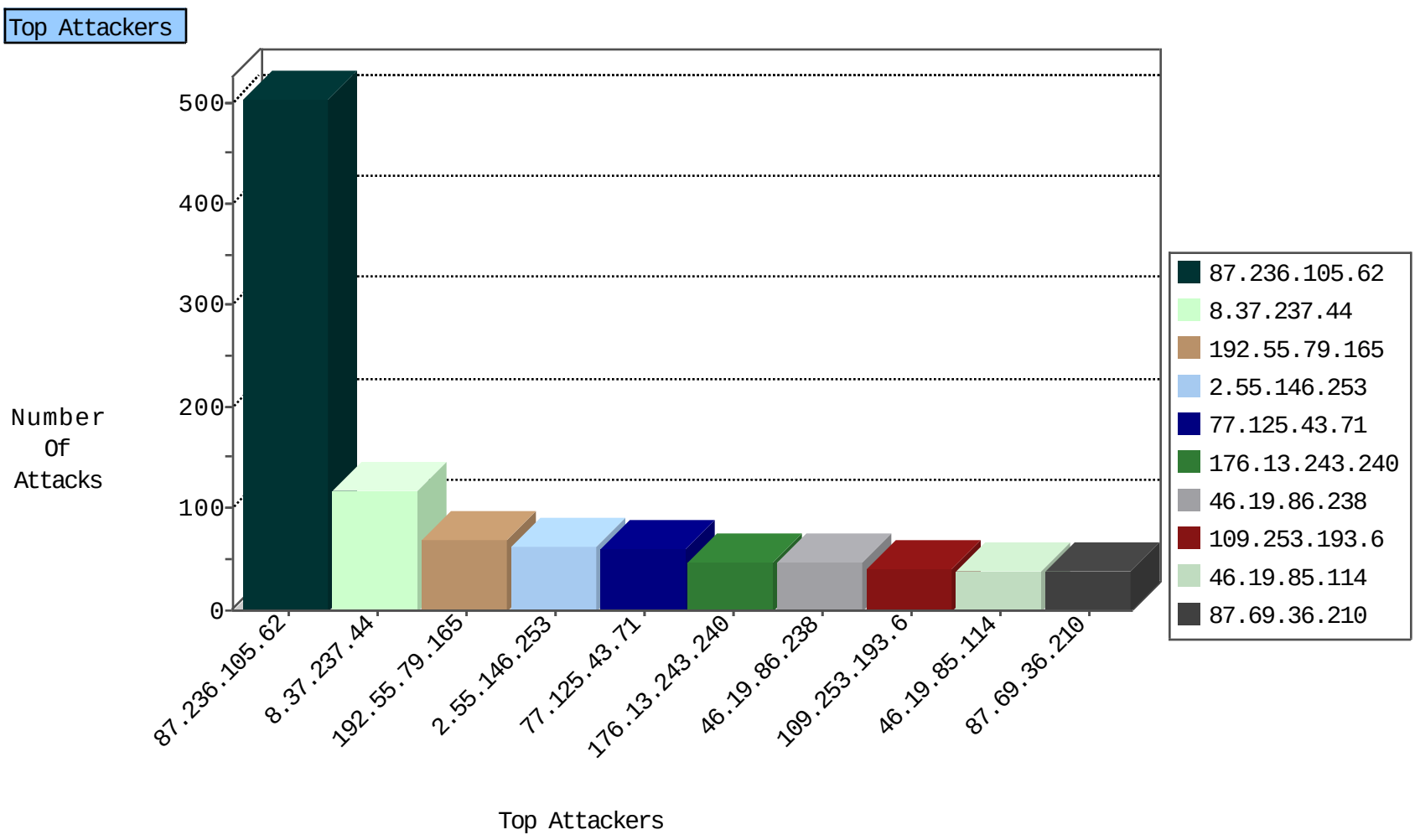
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-14-2016-08:04:05 to 09-14-2016-09:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.236.105.62	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	60
87.236.105.62	Germany	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	4
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
8.37.237.44	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
192.115.83.5	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
2.55.146.253	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.34	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
91.224.160.106	Netherlands	147.237.8.50	e.tikshuv.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
195.113.161.83	Czech Republic	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
192.33.90.68	Switzerland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.139	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
128.42.142.41	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-14-2016-08:04:05 to 09-14-2016-09:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	12
69.30.211.2	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4

09-14-2016-08:04:05 to 09-14-2016-09:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.224.160.106	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
77.139.168.208	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	2
91.224.160.106	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential SSH Scan	1
80.179.20.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	1
199.203.62.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
62.219.208.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
179.43.141.198	147.237.76.198	Switzerland	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
132.252.173.4	147.237.77.216	Germany	dover.idf.il	GPL SCAN nmap TCP	1
5.102.242.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
94.102.52.71	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
80.246.137.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN Potential SSH Scan	1
80.178.158.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
66.249.64.85	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	1
194.90.119.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
46.117.178.185	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
172.245.173.142	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
94.102.52.71	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1

09-14-2016-08:04:05 to 09-14-2016-09:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.236.105.62	Germany	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	418
8.37.237.44	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	115
87.236.105.62	Germany	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	78
192.55.79.165	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
77.125.43.71	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
207.232.54.210	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
176.13.230.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
2.55.146.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
46.19.86.238	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
46.19.85.114	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
216.72.40.185	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.86.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.85.114	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
109.253.206.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
82.80.196.44	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
2.55.146.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.55.146.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
91.197.61.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.55.146.253	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
185.127.10.35	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
2.55.146.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
87.69.36.210	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
87.69.36.210	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
5.246.41.85	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
207.46.13.85	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
87.69.36.210	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
212.179.218.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
59.189.233.81	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
176.13.243.240	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
138.134.192.10	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
176.13.243.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
176.13.243.240	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
185.127.10.35	Israel	147.237.72.167	ishurim.aka.idf.i	drop	SAM rule	drop	7
176.13.243.240	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
176.13.243.240	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
109.64.186.158	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.86.238	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
176.13.243.240	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
217.170.112.226	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.0.206.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.237	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.237	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.139	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
212.179.218.166	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.237	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.143	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.237	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.243.240	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.253.128.53	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.193.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
2.53.161.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
176.13.20.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
46.19.85.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
109.253.145.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.55.32.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.26.149.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.168.208	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	2
89.237.65.255	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/haredim/general.aspx	Block	2
80.246.133.90	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
207.232.54.210	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
46.19.86.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
208.54.5.216	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	2
2.53.174.114	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
114.97.198.63	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kapatz/default.aspx/trackback/	Block	1
87.69.39.132	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
62.90.122.237	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
213.151.63.166	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
176.13.5.25	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
8.37.237.168	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	1
109.197.22.206	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/yohalan	Block	1
77.138.136.159	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	Block	1
207.46.13.57	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.19.85.215	Israel	147.237.76.42	refuah.idf.il	Distributed Malformed URL	Block	1
2.53.178.182	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
141.226.218.114	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 141.226.218.114 (Open Mode)	None	1
87.69.39.132	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.9.6	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
176.13.10.30	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
46.19.85.215	Israel	147.237.76.42	refuah.idf.il	Distributed Unknown HTTP Request Method	Block	1
207.232.54.210	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
141.226.218.114	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.128	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/6/69406.pdf	Block	1
37.142.233.216	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$employmentStatus in www.aka.idf.il/main/sachar/payslips.aspx	None	1
2.53.7.141	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.215	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version	Block	1
8.37.237.168	United States	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
109.64.146.179	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.64.146.179	Block	1
66.249.64.181	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
185.3.147.181	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/rules.abe	Block	1
109.253.206.56	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	1
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
8.37.237.168	United States	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
157.55.39.196	United States	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
109.64.186.158	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.228.165	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
192.198.151.43	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/inner.asp	Block	1
46.19.85.215	Israel	147.237.76.42	refuah.idf.il	Distributed Abnormally Long Request	Block	1