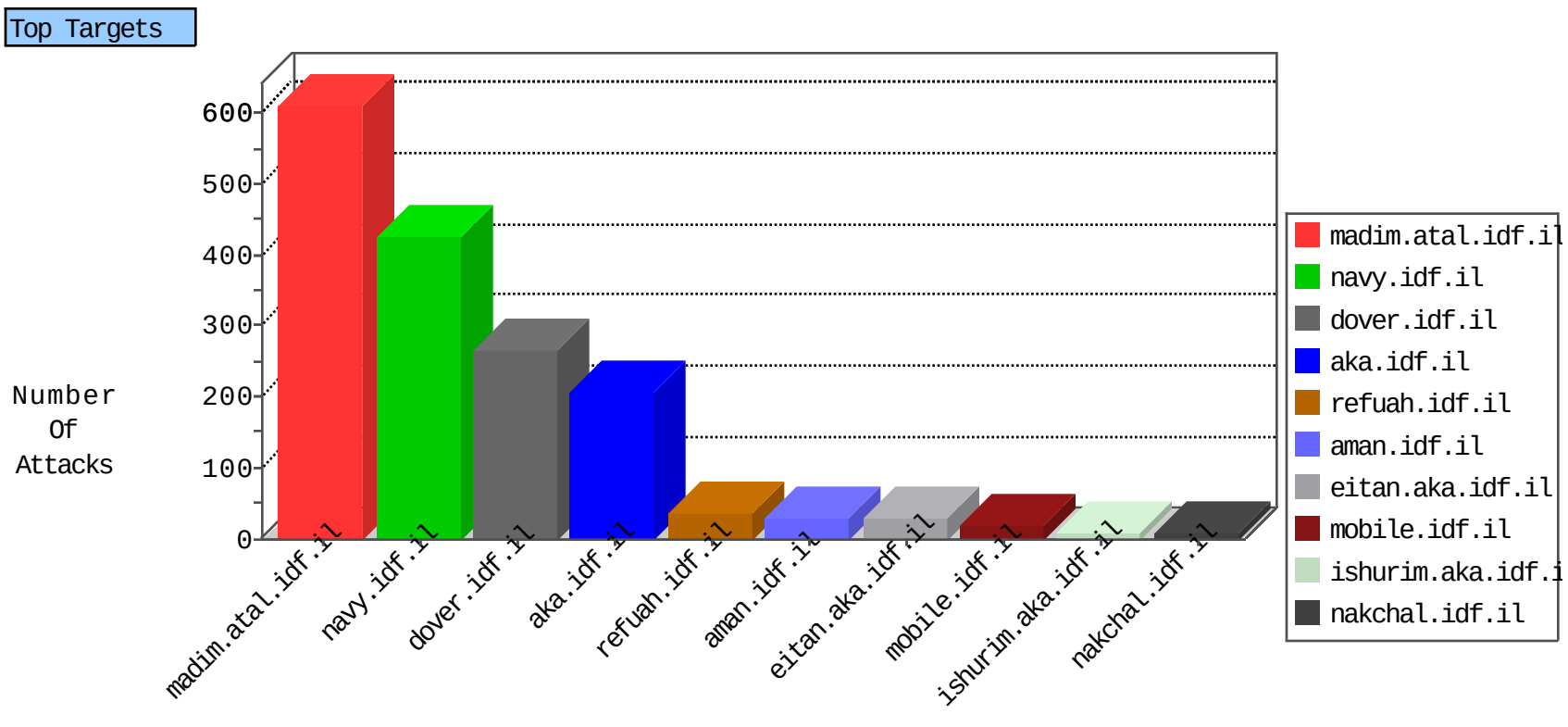
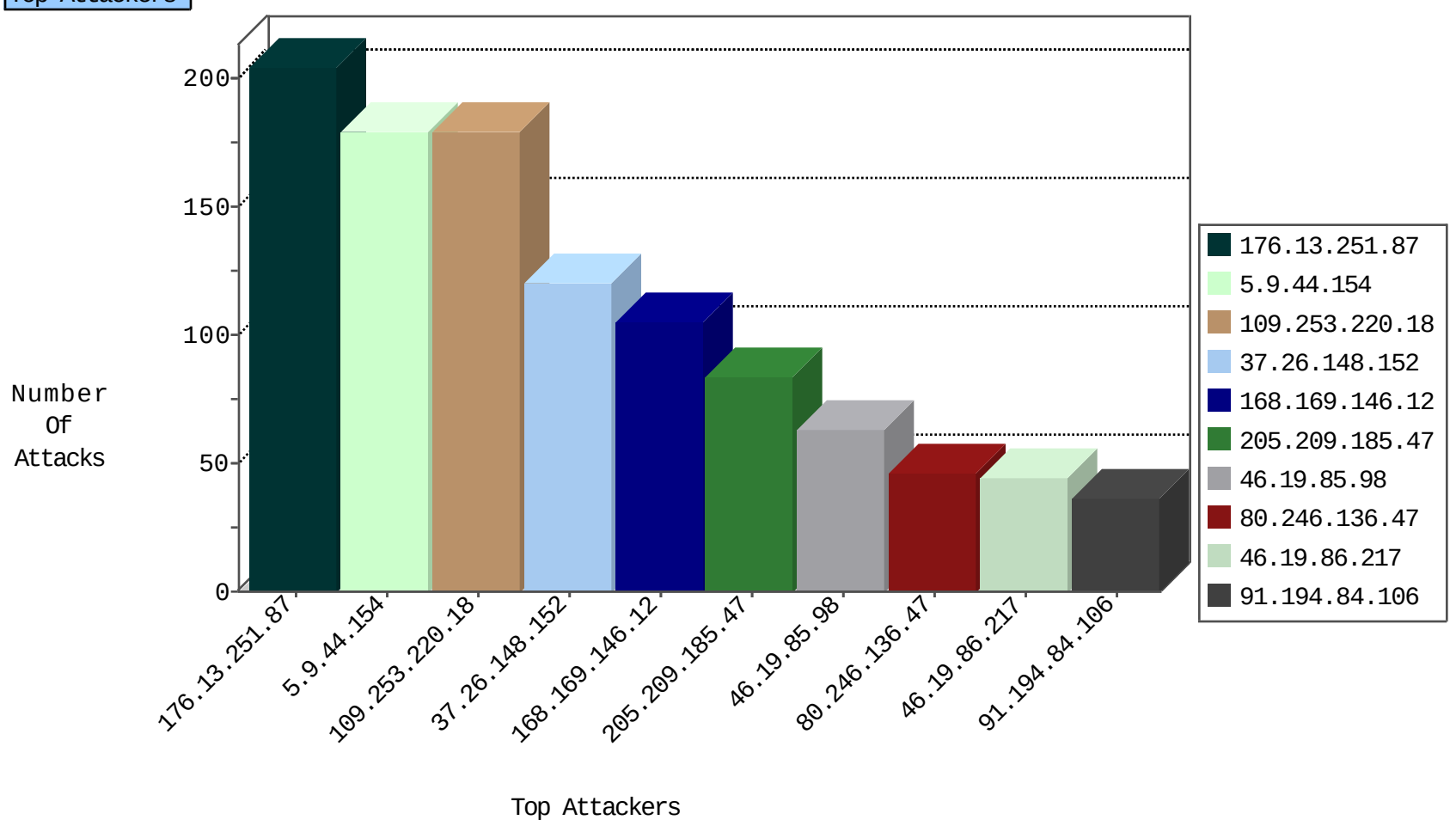
09-22-2016-16:04:01 to 09-22-2016-17:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-22-2016-16:04:01 to 09-22-2016-17:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.198.65	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
176.13.235.90	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
191.96.249.37	Chile	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
109.253.213.182	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
211.149.197.148	China	147.237.76.202	e.halag.idf.il	Black List	drop	1
191.96.249.34	Chile	147.237.76.38	e.e.meitav.idf.i	Black List	drop	1

09-22-2016-16:04:01 to 09-22-2016-17:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.194.84.106	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	34

09-22-2016-16:04:01 to 09-22-2016-17:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.253.192.217	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.120.29.172	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.94.7	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.90.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.155	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
24.173.213.138	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
5.29.133.224	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.183.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.166.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
211.149.244.79	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
87.69.180.174	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.203.172.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.25.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.227.84	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.138.243.23	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
146.200.148.0	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	1
62.219.113.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.144.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.111.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.60.153.178	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
31.154.9.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.155	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
5.102.254.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.197.232.2	147.237.77.212	Russian Federation	e.dover.idf.il	ET SCAN Potential SSH Scan	1
5.28.144.229	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.70.22.45	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.193.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
200.241.137.4	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
79.179.30.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.70.44.28	147.237.72.156	Hungary	aman.idf.il	ET SCAN NMAP -sS window 1024	1
79.176.91.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
147.236.232.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
64.137.168.128	147.237.76.34	Canada	yohalan.idf.il	ET SCAN Potential SSH Scan	1

09-22-2016-16:04:01 to 09-22-2016-17:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	180
168.169.146.12	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	105
205.209.185.47	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
205.209.185.47	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	18
205.209.185.47	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	18
46.19.86.217	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.86.217	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
205.209.185.47	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
109.253.211.152	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
205.209.185.47	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
37.26.147.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.26.146.148	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.178.147.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.86.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
84.229.8.189	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
132.70.66.12	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
84.229.8.189	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
155.254.215.14	Bahrain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
193.127.207.152	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
209.141.38.22	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	7
85.64.173.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.19.85.248	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
141.0.14.148	Europe	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
141.0.14.148	Europe	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
209.141.38.22	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
209.141.38.22	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.64.81	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.35.80.255	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.55.26.168	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.246.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
195.60.235.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.55.26.168	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
77.124.33.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.26.147.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.55.26.168	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
2.55.26.168	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
2.55.26.168	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
205.209.185.47	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
157.55.39.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.3.147.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.191	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
94.230.86.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.29.164.200	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
79.177.171.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.251.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	205
109.253.220.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	179
37.26.148.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	121
46.19.85.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
80.246.136.47	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.246.136.47	Block	27
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
46.19.85.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
46.19.85.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
82.208.100.206	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	4
37.188.134.125	Czech Republic	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	3
217.157.54.26	Denmark	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	3
194.78.217.148	Belgium	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 194.78.217.148	Block	3
2.53.131.223	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	3
104.131.160.127	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluiml	Block	2
2.53.137.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.94.152.251	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/he/navy.aspx	Block	2
5.28.176.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	2
87.69.222.132	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
212.235.34.10	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
94.243.218.98	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
194.78.217.148	Belgium	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/cityofficers/	Block	1
66.102.9.3	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
109.253.212.222	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
31.154.81.79	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
80.246.136.47	Israel	147.237.72.166	aka.idf.il	Unknown Parameter IMul in www.aka.idf.il/main/sachar/viewpayslip.aspx	None	1
46.19.85.207	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/brothers/news/default.asp	None	1
80.246.136.47	Israel	147.237.72.166	aka.idf.il	Unknown Parameter SlipIDMul in www.aka.idf.il/main/sachar/viewpayslip.aspx	None	1
207.46.13.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/brothers/gallery/	None	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/tizmoret/gallery/showpicture.asp	Block	1
80.246.136.47	Israel	147.237.72.166	aka.idf.il	Unknown Parameter Mul in www.aka.idf.il/main/sachar/viewpayslip.aspx	None	1
213.151.35.218	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
109.64.133.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.136.47	Israel	147.237.72.166	aka.idf.il	Unknown Parameter SlipIMul in www.aka.idf.il/main/sachar/viewpayslip.aspx	None	1
207.46.13.190	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
66.249.79.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-22454-he/idfgdover.aspx	Block	1
109.253.220.18	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtFirstName in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	1
85.64.94.150	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.136.47	Israel	147.237.72.166	aka.idf.il	Unknown Parameter SMul in www.aka.idf.il/main/sachar/viewpayslip.aspx	None	1
46.19.86.91	Israel	147.237.76.31	nakchal.idf.il	Malformed URL	Block	1
192.118.10.10	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	1
109.66.135.52	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
5.29.90.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
80.246.136.47	Israel	147.237.72.166	aka.idf.il	Unknown Parameter SlipMul in www.aka.idf.il/main/sachar/viewpayslip.aspx	None	1
212.179.159.253	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
79.177.231.36	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
140.147.236.195	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/giyus/general/	Block	1
80.246.136.47	Israel	147.237.72.166	aka.idf.il	Unknown Parameter SlMul in www.aka.idf.il/main/sachar/viewpayslip.aspx	None	1
46.19.86.91	Israel	147.237.76.31	nakchal.idf.il	Unknown HTTP Request Method q=0.4 in URL	Block	1
109.160.213.168	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1437-he/atal.aspx	Block	1