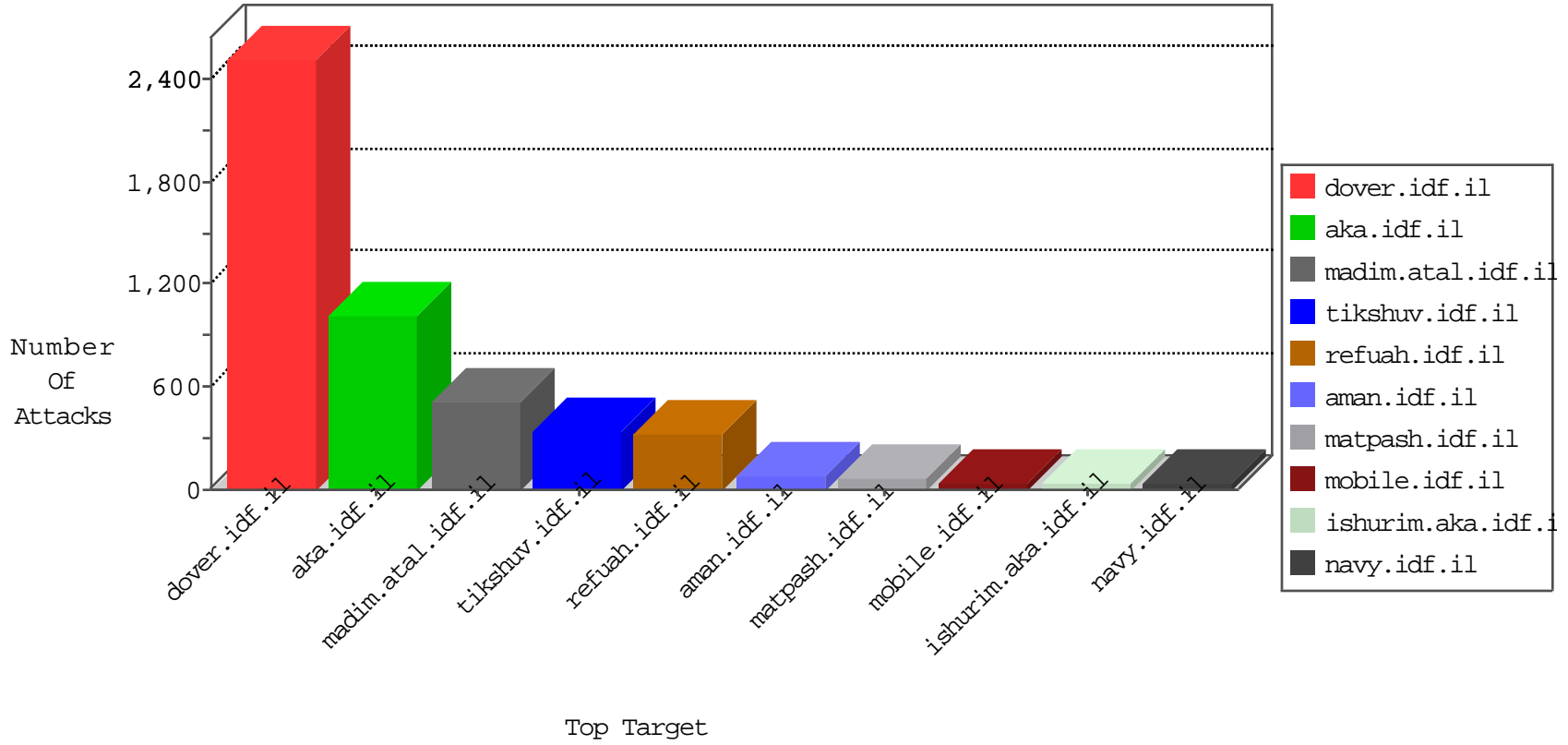


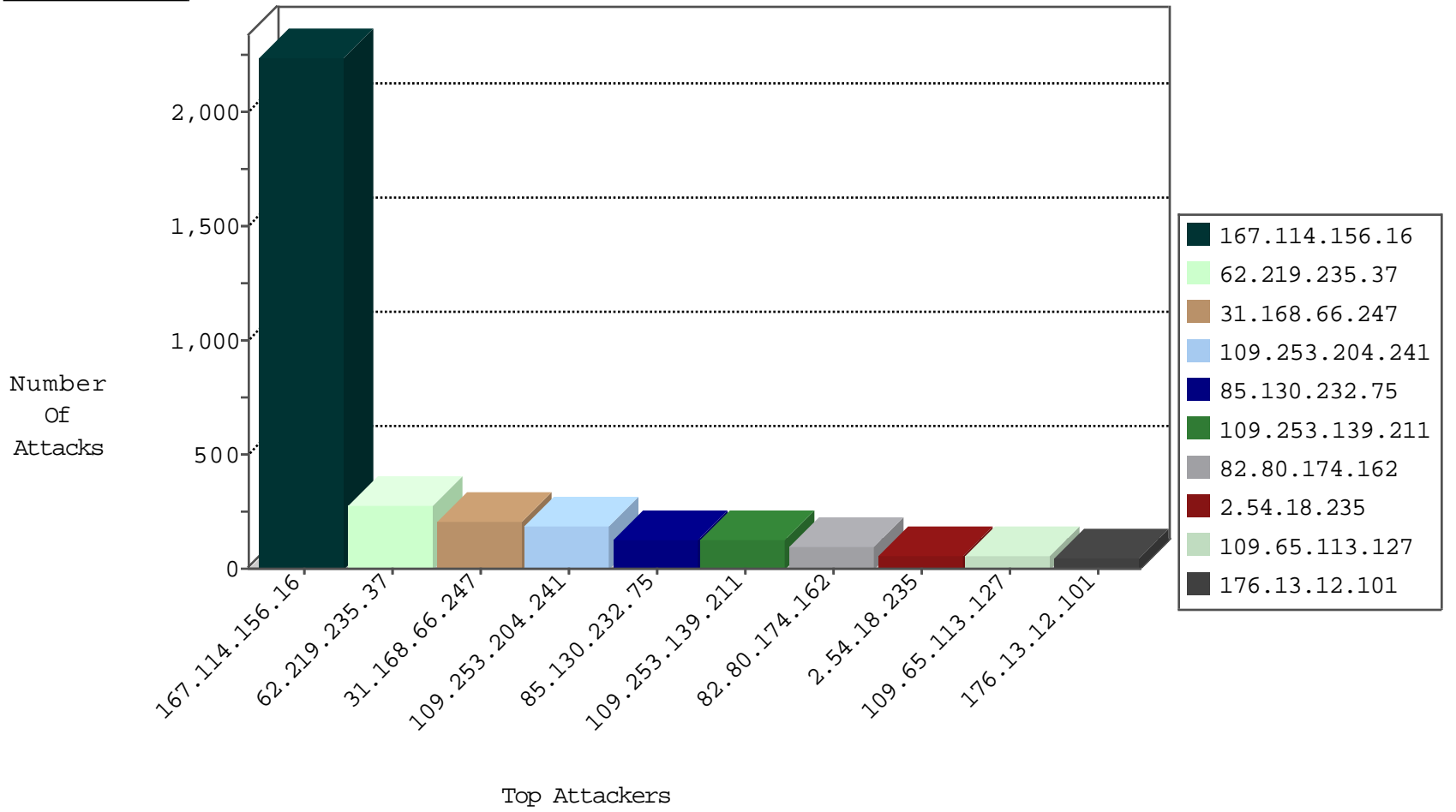
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4947
66.249.75.214	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	576
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
66.249.75.206	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	59
204.42.253.130	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	2
66.249.75.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1

01-05-2016-11:04:00 to 01-05-2016-12:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	C1000169: Block - dns poisoning (Clalit)	Permit	1

## 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	3
52.90.147.148	147.237.77.226	United States	www.chamatz.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
46.121.229.245	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.147.221	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.150.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
179.184.162.75	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.203	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
88.204.187.90	147.237.76.201	Kazakstan	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
79.181.57.192	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
52.90.147.148	147.237.76.38	United States	e.e.meitav.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
46.19.85.92	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
207.232.28.184	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.120.125.43	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
109.228.33.167	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
88.204.187.90	147.237.76.201	Kazakstan	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1
81.218.116.129	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.219.235.37	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	278
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	243
85.130.232.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	120
212.143.124.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
197.165.186.13	Egypt	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
202.159.140.198	Australia	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
62.0.197.69	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
46.19.86.31	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
62.0.214.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
185.120.126.73		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
46.19.86.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
212.235.103.211	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
2.54.18.235	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
46.19.85.147	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.54.18.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
2.54.18.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.18.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
2.54.18.235	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
88.175.64.221	France	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
66.249.64.250	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.86.176	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.96	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
94.230.86.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
195.160.240.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	9
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
37.26.146.181	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
185.120.126.73		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
2.52.41.156	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
176.13.8.224	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
132.73.195.190	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
31.154.135.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.182.254.8	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.182.254.8	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
62.90.131.58	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.182.231.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.64.146.173	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.235.62.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.182.254.8	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	7
149.88.97.161	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.12.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.78.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.142.64.26	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.204.241	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	181
31.168.66.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	99
82.80.174.162	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 82.80.174.162	Block	94
31.168.66.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	86
109.253.139.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	64
109.253.139.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	57
109.65.113.127	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	50
176.13.12.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	45
176.13.17.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
185.32.179.136	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
46.19.85.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
31.168.66.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	14
209.88.173.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/\$\$\$&?&?\$\$\$	Block	9
132.72.32.193	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 132.72.32.193	Block	9
80.246.139.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
176.13.4.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
2.52.14.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
194.90.128.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.128.185	Block	4
109.65.113.127	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	4
109.253.135.19	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.210.136.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
92.61.233.66	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 92.61.233.66	Block	3
46.19.85.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.16.143	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	3
46.19.86.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.6.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
192.116.190.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.228.233.164	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/tizmoret/faq/default.asp	None	2
37.26.147.129	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
212.179.132.201	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
46.19.85.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	2
46.19.85.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
199.207.253.101	United States	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtFirstName in www.refua.atal.idf.il/926-he/refuah.aspx	Block	2
46.19.85.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
132.64.26.121	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
37.26.146.175	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
194.90.254.244	Israel	147.237.72.166	aka.idf.il	Unknown Parameter utm_source in www.aka.idf.il/	None	1
2.54.59.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.69.233.18	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
176.13.21.140	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.248	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/w/load.php	Block	1
213.8.204.60	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.19.85.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.157.211	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.123.224	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct133 in www.aka.idf.il/main/sachar/payslips.aspx	None	1