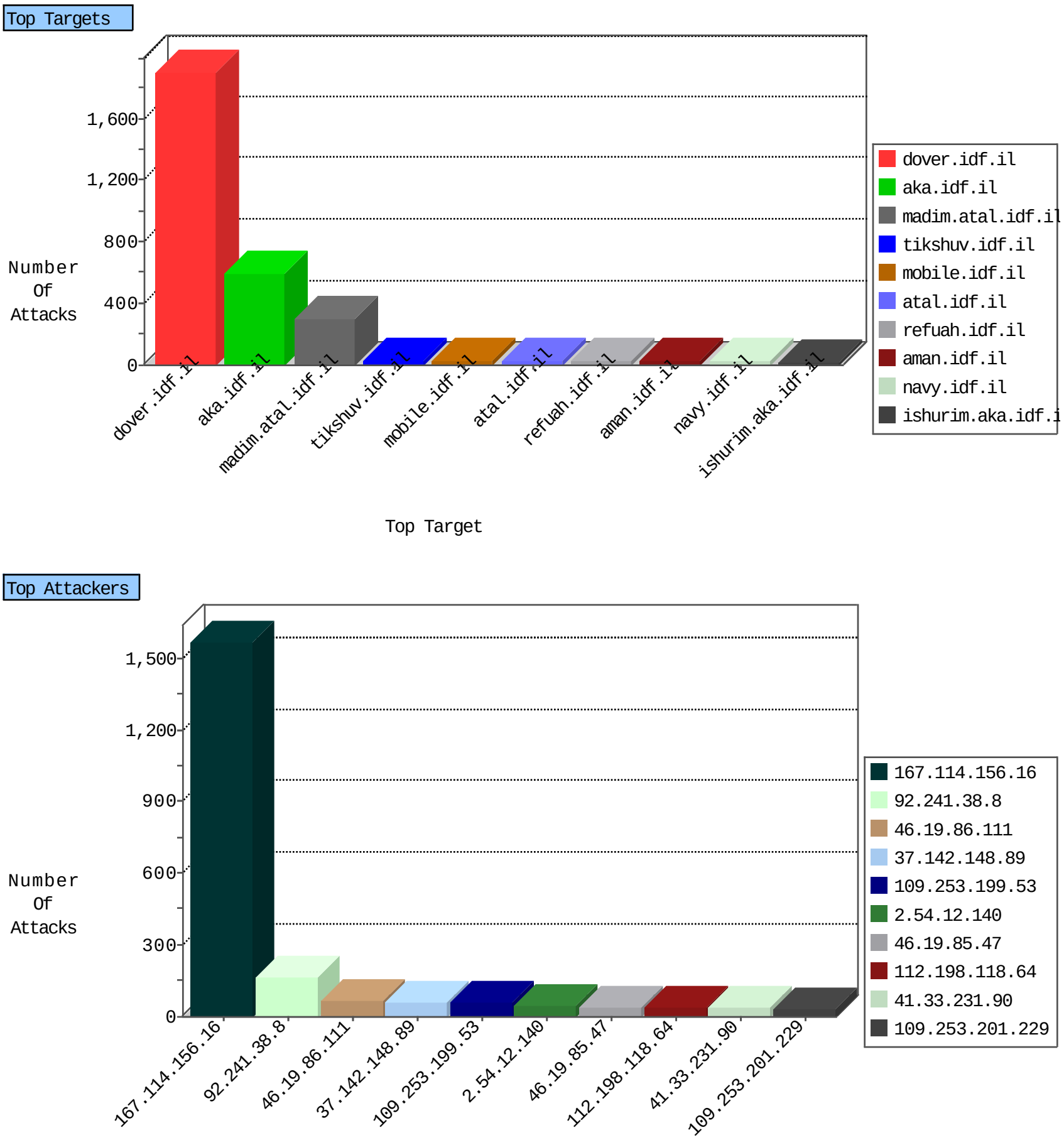
01-10-2016-17:04:04 to 01-10-2016-18:04:04

IDF Under Attack Daily Report



01-10-2016-17:04:04 to 01-10-2016-18:04:04

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	3028
185.126.176.195		147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
183.148.16.191	China	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
23.95.248.111	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
183.148.16.191	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1
183.148.16.191	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

01-10-2016-17:04:04 to 01-10-2016-18:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-10-2016-17:04:04 to 01-10-2016-18:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.179.103.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
54.72.0.55	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
158.255.6.220	147.237.76.38	Russian Federation	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.196	147.237.8.27	Netherlands	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
149.78.135.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.29.77	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.128.144.131	147.237.76.31	Canada	nakchal.idf.il	ET SCAN NMAP -f -sS	1
93.174.93.203	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.158.248	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.134	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
59.149.29.193	147.237.8.45	Hong Kong	e.eitan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
168.62.238.153	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
46.117.137.115	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.235.51	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.73.197.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.128.144.131	147.237.76.31	Canada	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.195	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.203	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
82.81.61.233	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

01-10-2016-17:04:04 to 01-10-2016-18:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
92.241.38.8	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	163
112.198.118.64	Philippines	147.237.72.166	aka.idf.il	drop	SAM rule	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	35
185.120.126.24		147.237.72.166	aka.idf.il	drop	SAM rule	drop	29
37.26.148.250	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
2.54.56.158	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
2.54.19.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
66.249.78.37	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
94.230.86.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
213.8.204.84	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
94.159.171.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
94.159.171.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
84.108.94.27	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.180.121.179	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	7
79.179.113.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.120.148.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.178.220.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.152.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.69.30	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.110	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
31.168.66.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
149.78.235.51	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	6
46.19.85.110	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.235.28.71	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.86.243	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.88.164.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.5	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
94.230.86.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.120.194.45	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
80.230.19.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.142.68.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.144.38	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
94.230.86.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.21.64	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.0.80.167	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
84.108.94.27	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.52.41.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
207.253.5.218	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.22.129.178	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.41.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
5.102.254.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.39.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.41.42	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
109.253.199.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
2.54.12.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
109.253.201.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
46.19.85.47	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	30
2.52.186.109	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 2.52.186.109	Block	22
176.13.21.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
84.95.251.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
84.108.224.206	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	7
80.246.136.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
207.46.13.123	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.123	Block	6
37.142.148.89	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 37.142.148.89	Block	5
37.142.148.89	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 37.142.148.89	Block	5
62.219.187.197	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	5
37.142.148.89	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 37.142.148.89	Block	5
79.178.152.84	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.178.152.84	Block	5
46.19.85.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
37.142.148.89	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 37.142.148.89	Block	5
37.142.148.89	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 37.142.148.89	Block	4
37.142.148.89	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 37.142.148.89	Block	4
37.142.148.89	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 37.142.148.89	Block	4
37.142.148.89	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 37.142.148.89	Block	4
192.0.80.167	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/rabanut/general.aspx	Block	4
37.142.148.89	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 37.142.148.89	Block	4
85.250.230.240	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
46.19.85.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.142.148.89	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
37.26.149.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.130	Block	3
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	3
176.13.21.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.20.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.136.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.69.242.104	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.242.104	Block	2
37.142.148.89	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 37.142.148.89	Block	2
80.246.136.232	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
37.26.146.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
95.86.93.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
37.26.146.200	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
85.250.87.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
81.65.170.19	France	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	2
176.13.23.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.133	Block	2
192.0.82.67	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/rabanut/general.aspx	Block	2
2.54.161.3	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1150-he/dover.aspx	Block	1
176.13.9.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.45.218	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.76.109.74	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.76.109.74	Block	1