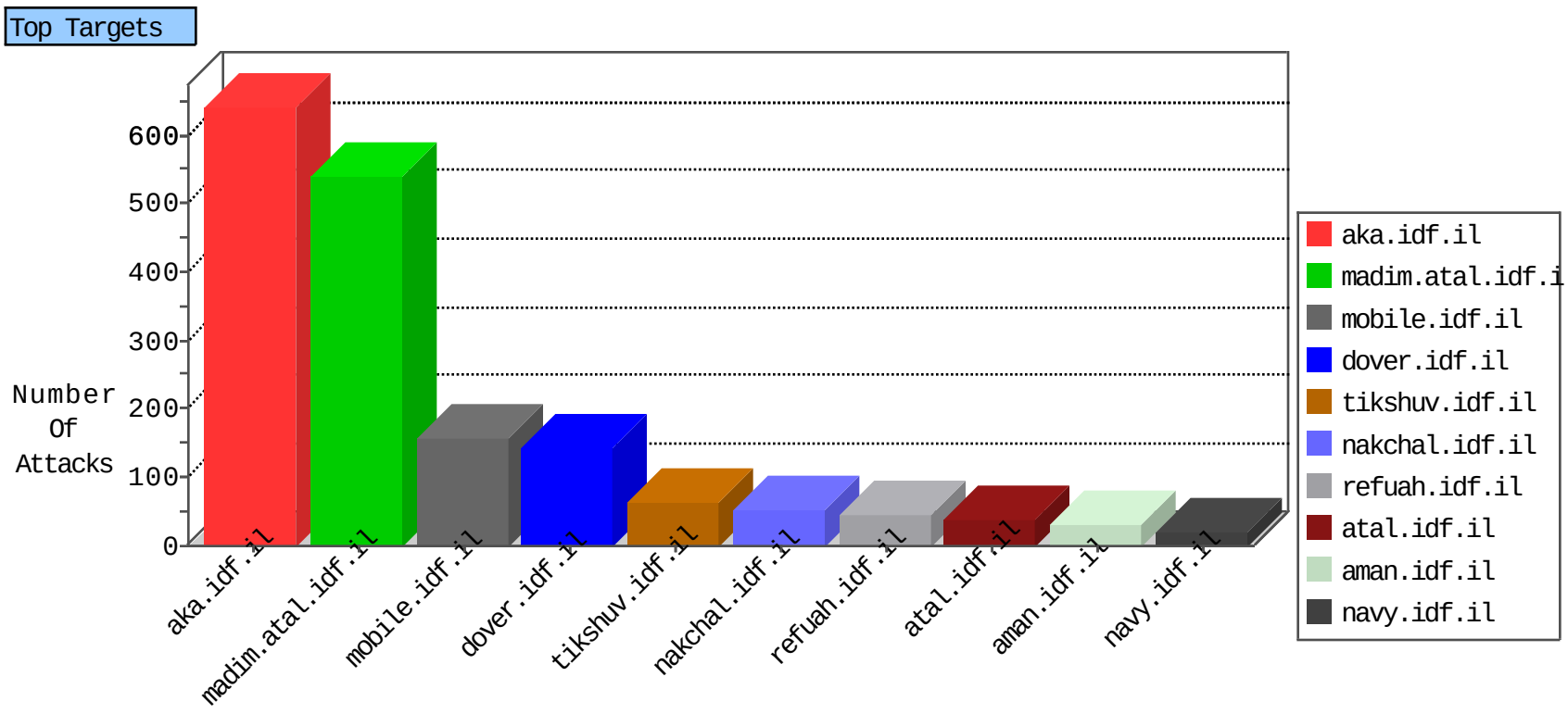
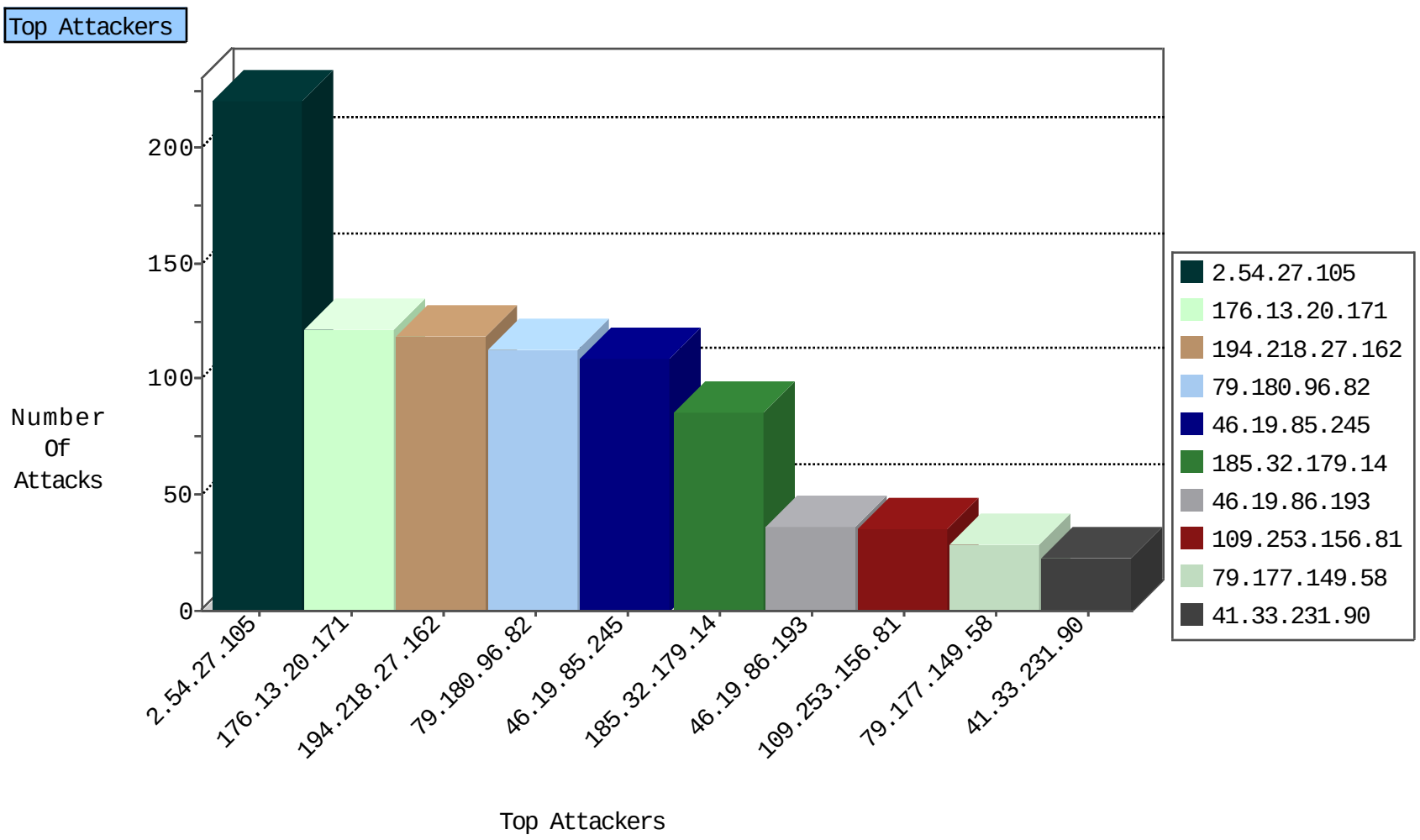
03-01-2016-15:04:08 to 03-01-2016-16:04:08

IDF Under Attack Daily Report





03-01-2016-15:04:08 to 03-01-2016-16:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.248.172.207	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
173.234.39.194	United States	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
113.222.45.36	China	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
173.234.39.194	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
84.228.199.122	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
173.234.39.194	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1

03-01-2016-15:04:08 to 03-01-2016-16:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.240	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
91.231.192.149	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
89.138.83.19	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
109.67.132.203	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
94.159.153.82	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
212.199.112.144	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
62.210.170.165	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	4
109.186.154.22	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
188.120.134.15	Israel	147.237.72.166	aka.idf.il	C1000008: HTTP: Xenu UserAgent	Block	2
5.29.86.179	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2

03-01-2016-15:04:08 to 03-01-2016-16:04:08

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	2
89.138.127.134	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.166.16.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.198.73	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.99.33	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.190.156	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.52.144.78	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
79.178.15.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.5.220.42	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.60.88	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.23.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.196	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.138.185.173	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.180.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.205.215	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.81.102.43	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.152.111	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.172.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.119.176	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.235.222	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
183.82.106.200	147.237.77.227	India	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
46.19.85.75	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.173.161.200	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.129.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

03-01-2016-15:04:08 to 03-01-2016-16:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	74
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	42
79.177.149.58	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
109.253.156.81	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
46.19.86.193	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	20
109.253.137.28	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.210.128.179	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
62.0.197.205	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
213.151.53.59	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
31.168.3.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.184	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.20.123	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.139.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.94	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
81.218.57.61	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.26.146.254	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
5.22.135.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
217.194.204.92	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
213.8.95.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.59.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.142.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.171.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.59.118	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.253.145.169	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.184.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.167.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.245	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.197.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.202.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.29.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.33.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.154.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.38.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.7.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.56.24	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.244.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
194.90.25.90	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
2.52.18.104	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.70.38.228	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5

03-01-2016-15:04:08 to 03-01-2016-16:04:08

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.86.193	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.242.253	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
89.139.177.145	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
89.139.252.170	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
84.228.199.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
2.52.48.243	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.27.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	170
176.13.20.171	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	122
46.19.85.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	101
185.32.179.14	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	86
2.54.27.105	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	51
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 192.115.64.250	Block	17
84.94.184.191	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
79.180.96.82	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	13
79.180.96.82	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	12
79.180.96.82	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	12
79.180.96.82	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 79.180.96.82	Block	10
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	10
79.180.96.82	Israel	147.237.72.166	aka.idf.il	Distributed Malformed URL	Block	10
46.19.85.83	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	9
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	8
109.253.156.81	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
79.180.96.82	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 79.180.96.82	Block	7
79.180.96.82	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 79.180.96.82	Block	7
79.180.96.82	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 79.180.96.82	Block	7
79.180.96.82	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 79.180.96.82	Block	7
79.180.96.82	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 79.180.96.82	Block	7
79.180.96.82	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 79.180.96.82	Block	6
2.54.179.94	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
31.168.13.41	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/894-he/refuah.aspx -	Block	4
79.180.96.82	Israel	147.237.72.166	aka.idf.il	Distributed NULL Character in Method	Block	4
79.180.96.82	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 79.180.96.82	Block	4
37.26.149.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
84.94.184.191	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	4
212.76.100.116	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.76.100.116	Block	3
31.154.94.50	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 31.154.94.50	Block	3
176.13.20.123	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
2.52.143.123	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.139.107	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.94	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.102.7.240	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
31.154.94.50	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	2
46.19.86.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.115.64.250	Block	2
79.180.96.82	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 79.180.96.82 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	2
212.76.100.116	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
46.19.86.184	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.245	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
87.70.38.228	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.180.96.82	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Parameter Name '‹Œh¨¦„ŋNDzÝ9,[[^'#20 ni ±]]|k„½¯T$c£°b[[#30]]Y†ÊÛ=$fy>0d^„[[#4]][[#25]]„¼„„seŸuœ*ad„ŽT mŋ]]#27[[¸]]#30[[]]#4[[]]#26[[°	Block	1
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/payslips.aspx	Block	1
79.180.96.82	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Illegal Byte Code Character in URL	Block	1
66.102.7.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.85	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/haredim/maslulimlist.aspx	Block	1