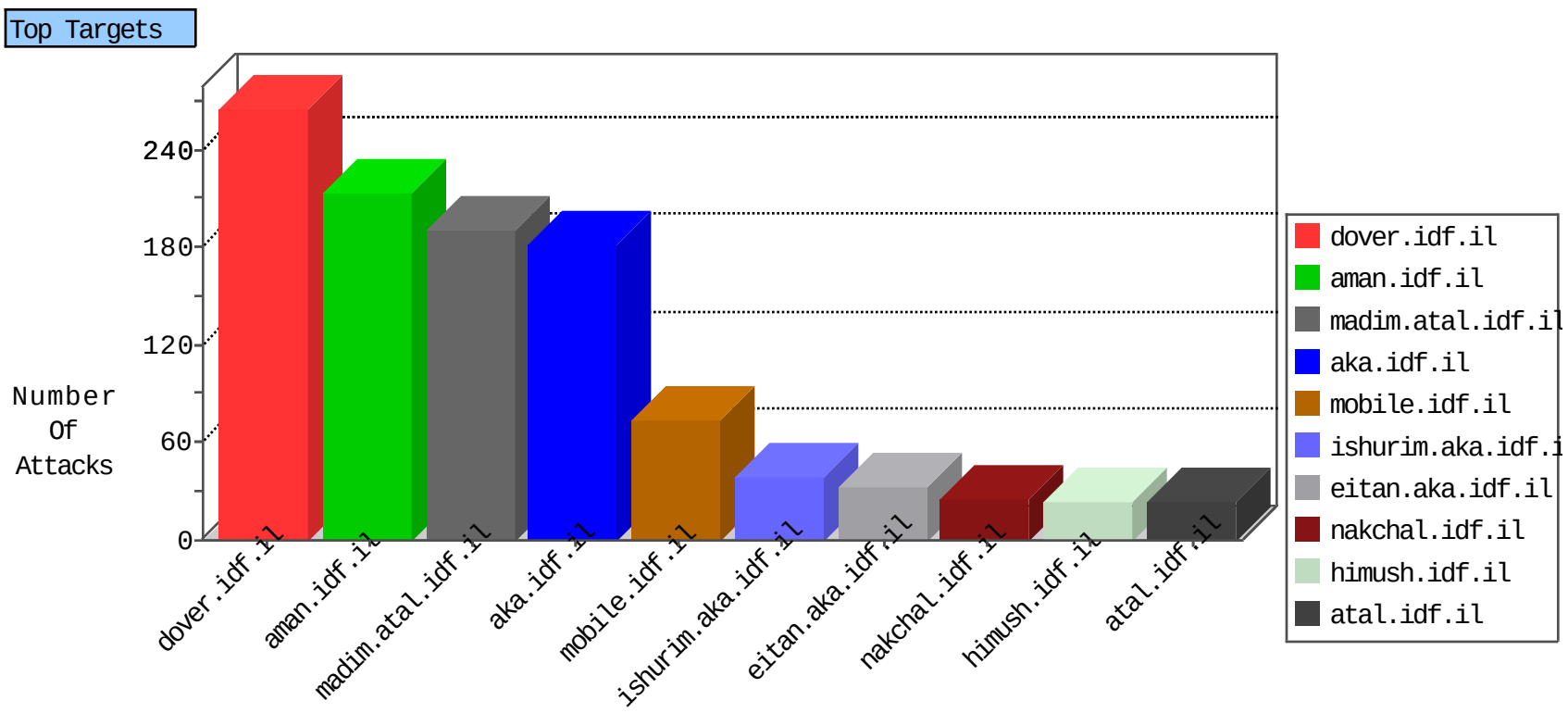
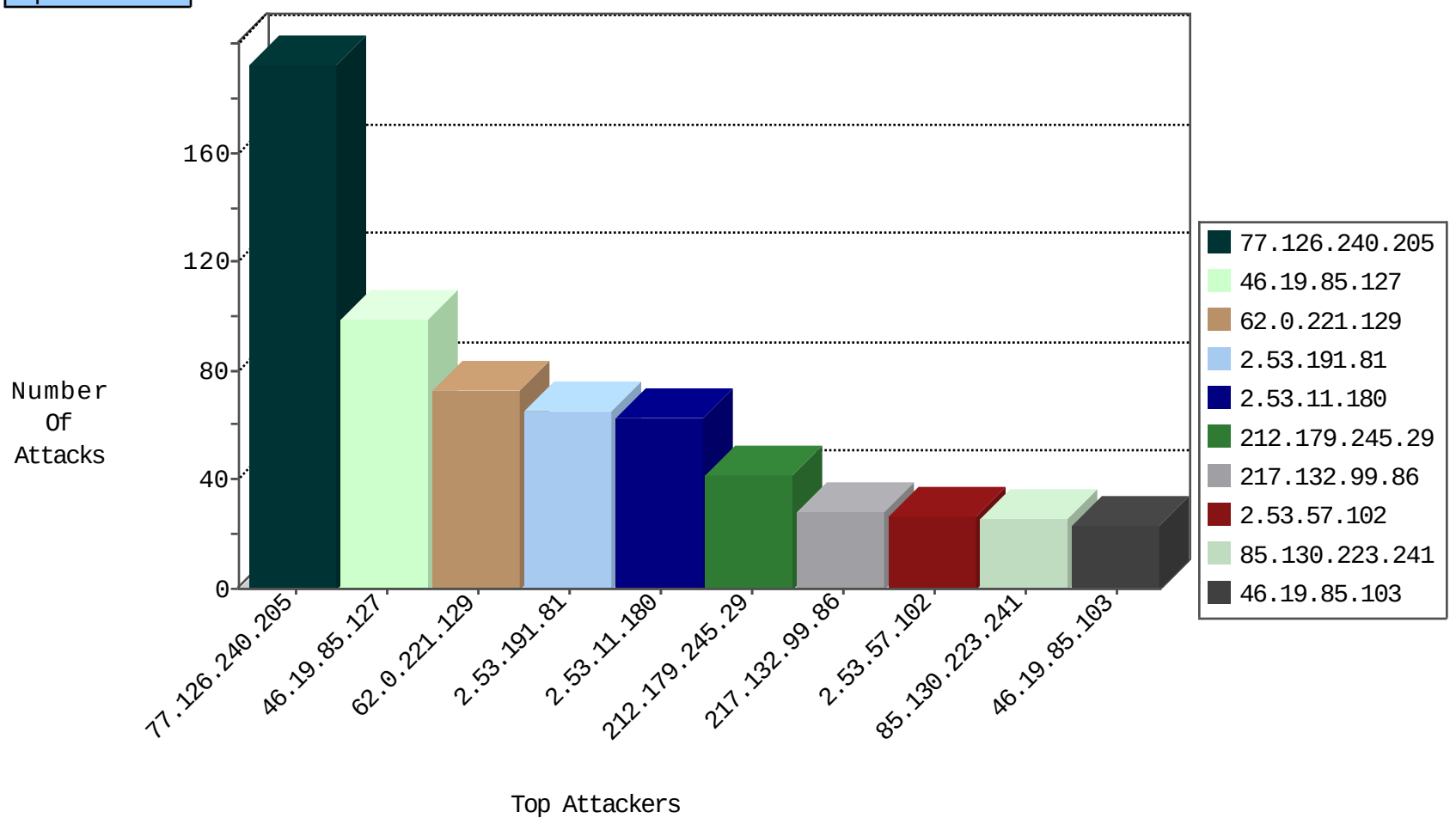
09-20-2016-13:04:02 to 09-20-2016-14:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-20-2016-13:04:02 to 09-20-2016-14:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.162	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
79.182.109.208	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-20-2016-13:04:02 to 09-20-2016-14:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-20-2016-13:04:02 to 09-20-2016-14:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
185.130.6.226	147.237.76.198	Lithuania	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
46.120.191.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.6.226	147.237.0.15	Lithuania	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.255	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.8.36	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.190	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.37.105	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.55.14.234	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.158	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
2.53.41.126	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.139.145.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.245.14.50	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
193.169.70.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.37.112	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.6.226	147.237.77.212	Lithuania	e.dover.idf.il	ET SCAN Potential SSH Scan	1
46.121.66.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.6.226	147.237.72.14	Lithuania	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
46.117.212.192	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.120.126.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
141.226.150.86	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.55.130.85	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.158	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
2.53.60.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.248.160.155	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.18.80	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
88.202.218.236	147.237.72.166	United Kingdom	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.41.221	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.83.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.120.148.152	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
69.175.7.162	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

09-20-2016-13:04:02 to 09-20-2016-14:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
62.0.221.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
2.53.11.180	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
217.132.99.86	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
2.53.57.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
62.0.221.129	Israel	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	24
212.179.245.29	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
141.0.13.223	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
212.179.245.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
79.180.166.89	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
2.53.174.101	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
207.241.229.68	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
62.0.224.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
192.117.148.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
85.130.223.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
85.130.223.241	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
85.130.223.241	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
62.0.225.254	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.50	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.3.147.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
172.252.126.227	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
199.203.215.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.68	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.24.213	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.86.173	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
82.81.7.178	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.253.197.249	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
2.53.24.213	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
109.253.145.86	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence		alert	4
2.53.24.213	Israel	147.237.77.216	dover.idf.il	drop		drop	4
46.116.4.231	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.245.158	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
109.253.145.86	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence		monitor	4
46.19.85.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.26.149.143	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
176.13.19.112	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
62.44.134.178	Denmark	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.149.175	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.69.32.22	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
185.32.179.73	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
2.53.181.2	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.208.20	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.24.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	99
2.53.191.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 77.126.240.205	Block	24
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Distributed Malformed URL	Block	22
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Distributed Unknown HTTP Request Method	Block	21
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Distributed Abnormally Long Request	Block	18
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Name from 77.126.240.205	Block	15
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in URL from 77.126.240.205	Block	15
2.53.11.180	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
2.53.13.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple Illegal HTTP Version from 77.126.240.205	Block	12
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Header Line from 77.126.240.205	Block	10
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple NULL Character in Header Name from 77.126.240.205	Block	10
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple Malformed HTTP Header Line from 77.126.240.205	Block	9
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Value from 77.126.240.205	Block	9
176.13.251.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple NULL Character in Url from 77.126.240.205	Block	4
37.26.148.220	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	4
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple Illegal URL Path Encoding from 77.126.240.205	Block	4
109.253.222.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.120.156.98	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple NULL Character in Method from 77.126.240.205	Block	3
46.19.85.138	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
172.252.126.227	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/miluim/about.aspx	Block	2
87.71.25.221	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
118.8.27.72	Japan	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	2
2.53.57.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.8.204.27	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.85.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.57.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
77.139.177.35	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	2
46.120.201.154	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
185.46.214.84	Switzerland	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 185.46.214.84	Block	1
2.53.148.239	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Illegal URL Path Encoding •[[#31]]·xŠ[[#21]]9«↱—-[[#22]]ר•Œ 9[[#8]][[#17]]½¨[[#8]]¸$	Block	1
79.180.166.89	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
66.102.9.22	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
212.179.245.29	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Parameter Name .¸±[[#16]]Ü[[#29]]גנסז′ @¯{8Þc:¸®-[[#28]]@6Q[[#24]]P,u¯ in [[#19]][[#28]][[#4]]@Œ‹¢ך $ß7[[#4]]moוו_*§¤%m[[#23]]•[[#27]]•c»[['ו#24[[˜¢ו“פ*]]#27[[]]#11)]]	Block	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.69.126	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
46.19.85.220	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
185.46.214.84	Switzerland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/italian/	Block	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Malformed HTTP Header Line 2	Block	1
84.109.235.203	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
66.249.64.122	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
212.199.65.218	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 77.126.240.205 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Parameter Name from 77.126.240.205	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1