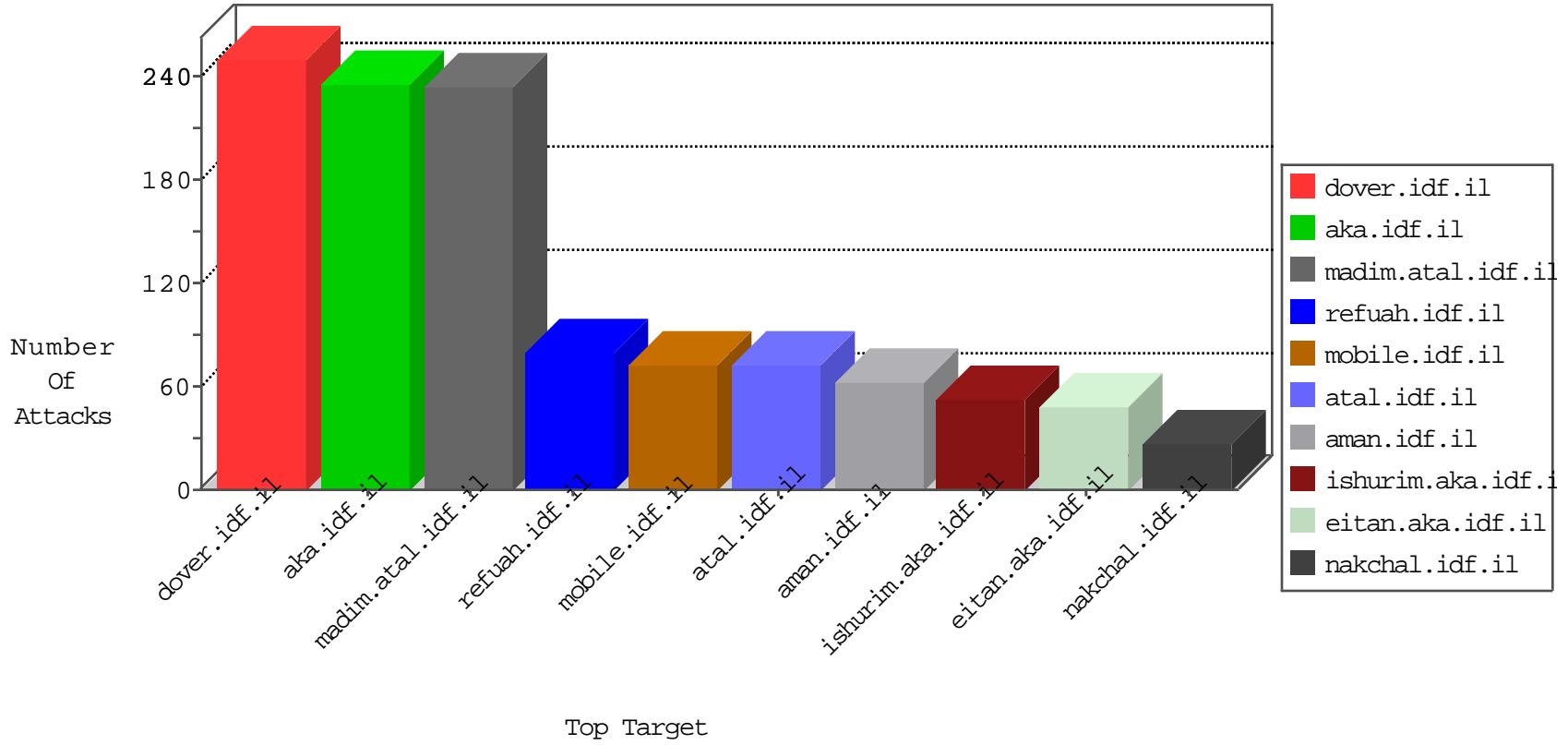


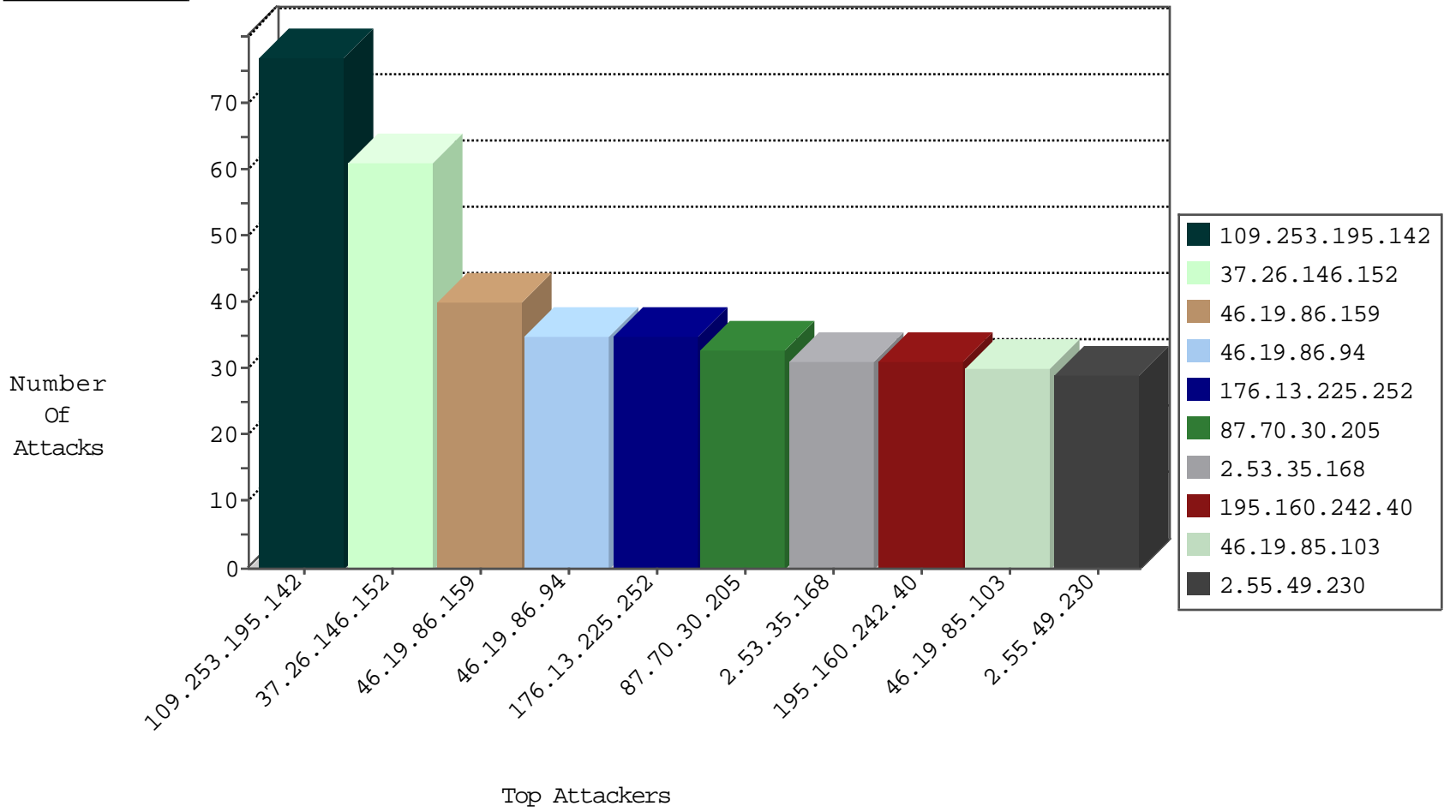
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
109.67.240.132	Israel	147.237.72.166	aka.idf.il	Black List	drop	2
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
109.123.125.158	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
192.33.90.68	Switzerland	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
131.179.150.72	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.1.13.12	Ireland	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
109.123.125.156	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
109.123.125.157	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
192.33.90.67	Switzerland	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.102.6.113	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	25
46.19.85.160	147.237.72.156	Israel	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	3
31.168.75.55	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	2
2.53.13.141	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.217.129.249	147.237.77.216	Netherlands	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.70.241	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
66.102.6.117	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.45.242.194	147.237.0.33	United States	idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
192.117.153.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.218.200.137	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
109.67.218.196	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.29.248	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.151.169	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.158.244	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.93.5.70	147.237.77.243	United Arab Emirates	mobile.idf.il	ET SCAN Potential SSH Scan	1
82.81.193.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.139.59.145	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.170.151	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
197.161.154.175	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.244.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.211.153	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.66.82	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.190.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.0	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.42.172	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.60.153.178	147.237.72.14	Russian Federation	dover.idf.il(ol	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.55.49.230	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
109.67.98.189	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	22
82.81.63.112	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
79.177.81.37	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
109.64.50.209	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
46.19.85.202	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	18
87.70.30.205	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
87.70.30.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
31.168.75.55	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
176.13.225.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.86.159	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.53.13.51	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.159	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
100.92.63.229		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.103	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.103	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.132	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
46.19.86.186	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
176.13.244.89	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.194.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
207.232.21.125	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.86.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
79.181.249.93	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.86.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.13.225.252	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
176.13.225.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.86.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
2.54.98.196	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.94	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.61	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
176.13.225.252	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
81.218.82.131	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	5
81.218.82.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.60	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.227	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.55.185.122	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.218	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.55.185.122	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
79.181.117.162	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.60	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
82.217.129.249	Netherlands	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.210.168.223	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
5.29.6.202	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.195.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
37.26.146.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
2.53.35.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
46.19.86.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
37.26.147.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
46.19.85.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
46.19.86.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.53.164.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
2.55.49.230	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
195.160.242.40	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	4
195.160.242.40	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 195.160.242.40	Block	3
79.182.84.188	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/guyus	Block	3
2.55.176.204	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.246.138.162	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/gyus	Block	2
77.138.131.83	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	2
46.121.37.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
77.139.85.185	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	2
109.253.194.131	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
77.138.131.83	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
80.246.138.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.222.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.168.164.198	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
31.168.164.198	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Value from 31.168.164.198	Block	1
212.179.21.194	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
77.139.34.214	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/smalim/smalim.aspx	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
31.168.164.198	Israel	147.237.72.156	aman.idf.il	Abnormally Long Request method	Block	1
176.13.229.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.172.0.104	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
37.26.149.178	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.177.152.192	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
31.168.164.198	Israel	147.237.72.156	aman.idf.il	Multiple Unknown HTTP Request Method from 31.168.164.198	Block	1
31.168.164.198	Israel	147.237.72.156	aman.idf.il	Illegal HTTP Version	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1
10.148.20.19		147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/sachar	Block	1
157.55.39.4	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
46.19.86.172	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
31.168.164.198	Israel	147.237.72.156	aman.idf.il	Unknown HTTP Request Method Ū[[#25]]µ[[#28]]"*[[#23]]•nâiJG[[#21]]oMzPøÅ. [[#31]]6@~[[#22]]Èf rō	Block	1
82.81.63.112	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
77.139.71.224	France	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$LoginControl\$captcha\$captchaText in www.aka.idf.il/main/gyus/default.aspx	None	1
31.168.164.198	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 31.168.164.198	Block	1
212.199.154.194	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/buttonback.png	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteyerua/	Block	1
31.168.164.198	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Name @JÛñ4ã;Vkt@[[#31]]èôç~*%ôlè...øÅG'	Block	1
176.13.241.5	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
106.38.241.105	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.85.171	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
79.177.152.192	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct155 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
31.168.164.198	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 31.168.164.198 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
31.168.164.198	Israel	147.237.72.156	aman.idf.il	Malformed URL >È0>q z[[#18]]epw [[#28]] h g š µ#012 f[[#26]]+dn[[#5]]k [[#8]]'7[[#27]][[#30]]bhuf@h²b]k[[#14]]™& [[#6]]p • o=)[[#24[[#27m]] ¶!> \!²[[12#]]^• ~ g]]7#[[#p'l... ,,,[[19#]]]{]]2#[[#s #kg•Èvaüxwš\$ x/[[#22]][[#28]]èxü , .-	Block	1