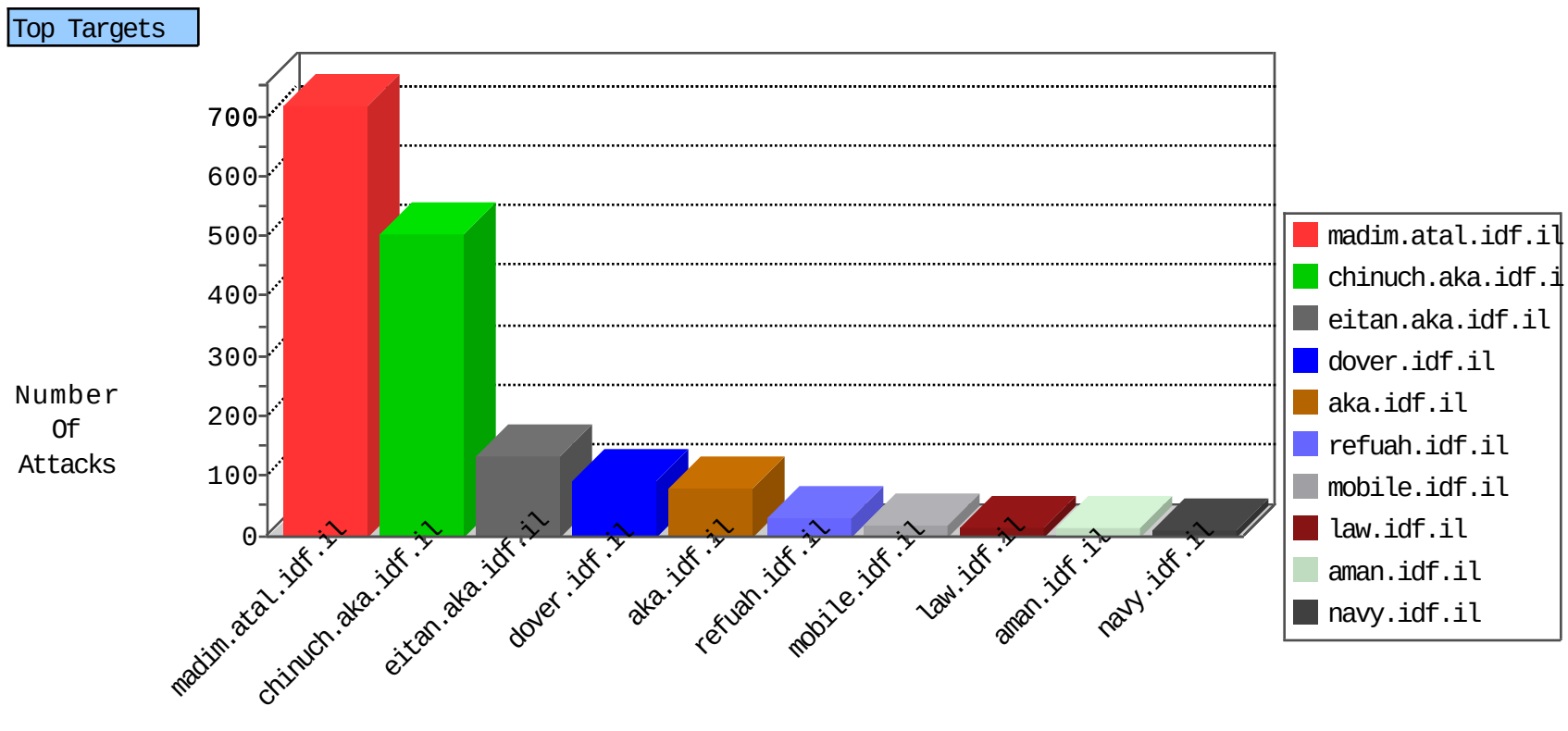
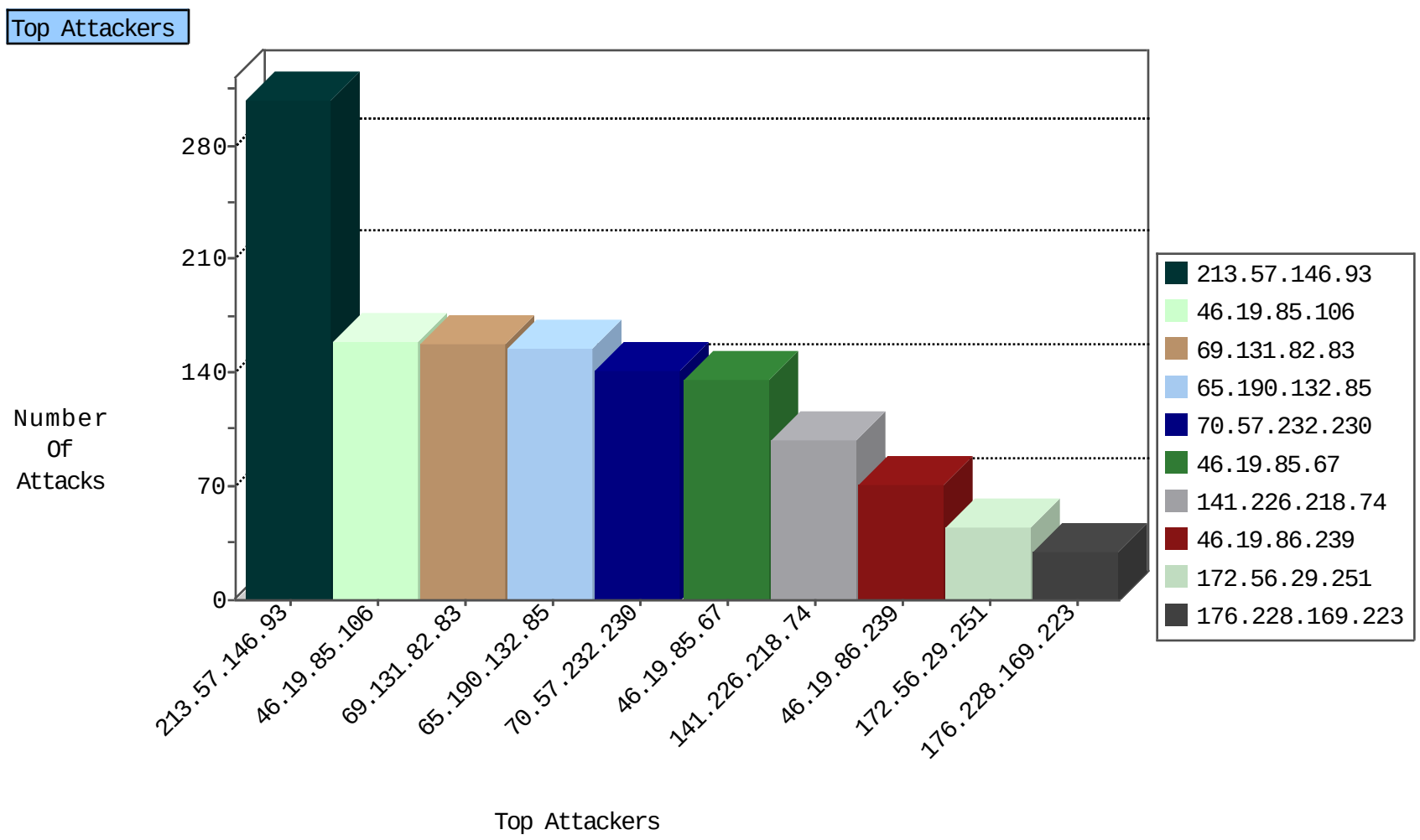
09-24-2016-15:04:08 to 09-24-2016-16:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-24-2016-15:04:08 to 09-24-2016-16:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.226.218	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
183.60.48.25	China	147.237.76.198	e.yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
204.12.220.83	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
31.204.128.22	Netherlands	147.237.76.34	yohalan.idf.il	Black List	drop	1
123.59.59.52	China	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
63.141.231.194	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
63.141.242.196	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
204.12.220.83	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1

09-24-2016-15:04:08 to 09-24-2016-16:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.149.132.179	Italy	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6

09-24-2016-15:04:08 to 09-24-2016-16:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.149.132.179	147.237.77.74	Italy	law.idf.il	SQL Injection - Select From	8
93.70.141.81	147.237.76.200	Italy	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
93.70.141.81	147.237.76.196	Italy	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
93.70.141.81	147.237.76.44	Italy	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
93.70.141.81	147.237.76.39	Italy	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	2
93.70.141.81	147.237.77.212	Italy	e.dover.idf.il	ET SCAN Potential SSH Scan	2
82.76.111.239	147.237.76.200	Romania	eitan.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
78.129.171.173	147.237.76.148	United Kingdom	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
185.129.148.230	147.237.0.34	Latvia	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
61.131.58.91	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
179.43.141.221	147.237.8.28	Switzerland	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
45.63.28.189	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
115.75.251.16	147.237.77.233	Vietnam	atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
14.220.65.204	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.70.141.81	147.237.77.234	Italy	halag.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.76.42	Ukraine	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
93.70.141.81	147.237.77.179	Italy	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.76.42	Ukraine	refuah.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
93.70.141.81	147.237.77.121	Italy	e.navy.idf.il	ET SCAN Potential SSH Scan	1
84.19.27.67	147.237.76.202	Germany	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
93.70.141.81	147.237.77.61	Italy	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
202.57.4.194	147.237.77.243	Indonesia	mobile.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.70.141.81	147.237.76.202	Italy	e.halag.idf.il	ET SCAN Potential SSH Scan	1
179.43.141.221	147.237.76.148	Switzerland	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
93.70.141.81	147.237.76.198	Italy	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
46.161.40.17	147.237.77.170	Russian Federation	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
122.3.129.138	147.237.76.42	Philippines	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.70.141.81	147.237.76.86	Italy	navy.idf.il	ET SCAN Potential SSH Scan	1
45.63.28.189	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
93.70.141.81	147.237.77.235	Italy	sviva.idf.il	ET SCAN Potential SSH Scan	1
93.70.141.81	147.237.76.42	Italy	refuah.idf.il	ET SCAN Potential SSH Scan	1
93.70.141.81	147.237.77.233	Italy	atal.idf.il	ET SCAN Potential SSH Scan	1
93.70.141.81	147.237.76.34	Italy	yohalan.idf.il	ET SCAN Potential SSH Scan	1
93.70.141.81	147.237.77.205	Italy	prisha.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.76.42	Ukraine	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
93.70.141.81	147.237.77.176	Italy	matpash.idf.il	ET SCAN Potential SSH Scan	1
84.19.27.67	147.237.76.202	Germany	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
93.70.141.81	147.237.77.74	Italy	law.idf.il	ET SCAN Potential SSH Scan	1
84.19.27.67	147.237.76.202	Germany	e.halag.idf.il	ET SCAN NMAP -f -sS	1
93.70.141.81	147.237.77.19	Italy	law-forum.idf.il	ET SCAN Potential SSH Scan	1

09-24-2016-15:04:08 to 09-24-2016-16:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
69.131.82.83	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	158
65.190.132.85	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	156
70.57.232.230	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	141
141.226.218.74	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
172.56.29.251	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	45
141.226.218.21	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
185.137.19.158		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.119	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.120.130.68	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
106.39.60.187	China	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	9
79.181.169.253	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
176.13.16.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.81	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.53.23.227	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.16.97	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
176.13.16.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.177.135.12	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
141.226.217.76	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.117.107.42	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
77.139.50.126	France	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.182.120.6	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
87.70.9.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.1.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
119.160.128.55	Brunei Darussalam	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
101.184.159.194	Australia	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
87.69.235.82	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.117.134.166	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.55	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.19.85.244	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
109.64.129.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
109.66.20.206	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
95.35.85.103	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.49	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.29.29.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
31.168.172.138	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.86.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.73	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
79.180.82.98	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.226.218.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.102.195.21	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
120.132.67.190	China	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.86.119	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.64.129.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.146.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	309
46.19.85.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	160
46.19.85.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	136
46.19.86.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
176.228.169.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
46.19.86.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
77.139.163.107	France	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 77.139.163.107	Block	5
176.13.13.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.163.107	France	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 77.139.163.107	Block	3
77.139.163.107	France	147.237.72.166	aka.idf.il	Multiple Malformed URL from 77.139.163.107	Block	3
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	3
77.139.163.107	France	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 77.139.163.107	Block	3
77.139.163.107	France	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 77.139.163.107	Block	3
77.126.8.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.163.107	France	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 77.139.163.107	Block	2
37.142.2.146	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	2
65.49.173.132	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	2
66.249.64.17	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to chinuch.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
46.19.86.40	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.139.163.107	France	147.237.72.166	aka.idf.il	Illegal HTTP Version èœ[[#16]]ÓoŸKMÁ-WŒ[[#25]]åçÃ’¹Q[[#12]]•ž¢äÉWÚD[[#26]]	Block	1
66.249.75.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1846-he/dover.aspx	Block	1
213.133.110.35	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
109.65.187.222	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/edim/theproj/theproj.asp	Block	1
46.117.176.107	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/general.aspx	None	1
31.168.1.202	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.138.7.248	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
66.249.64.108	Israel	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1
77.139.163.107	France	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 77.139.163.107 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
77.139.163.107	France	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 1	Block	1
66.249.75.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1362-9916-he/dover.aspx	Block	1
109.66.106.160	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.121.252.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/pniotfindanswer.aspx/	Block	1
77.139.163.107	France	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
66.249.65.52	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding aI_;fAQ&e>{GbP6@ywx@zx!d/u58^O/QN){GDx1akZ.v{MDZ42FdE_vwL-@_o)3ii;1 in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
213.8.204.11	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
77.139.163.107	France	147.237.72.166	aka.idf.il	NULL Character in Method „[[#25]]çjûzK <á{g8×G²gÊ[[#19]]~ü•"F'Û7*>[[#25]][[#24]]DË(¹?î(4˜¼Ï÷,¯•g [[#0]]‰[[#8]]£+_½ÐEf	Block	1
77.139.163.107	France	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 77.139.163.107	Block	1
66.249.75.42	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
141.226.218.21	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
77.139.163.107	France	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
213.8.204.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
84.229.52.25	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
46.116.125.169	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.76.113	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	1
157.55.39.121	United States	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
77.139.163.107	France	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 77.139.163.107	Block	1
77.139.163.107	France	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL ҂ÙtÌ¼‹´+¸©ƒ·\[[#3]]3,[g¸•/Ê¨[´′⁋]]22#[[v¨eˆûuƄÞ]]=72#Ð[[aiÞ…ɔ(e]]••.″2#]][[12#[[210#	Block	1
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
84.229.52.25	Israel	147.237.72.166	aka.idf.il	Unknown Parameter y in www.aka.idf.il/main/sachar/payslips.aspx	None	1