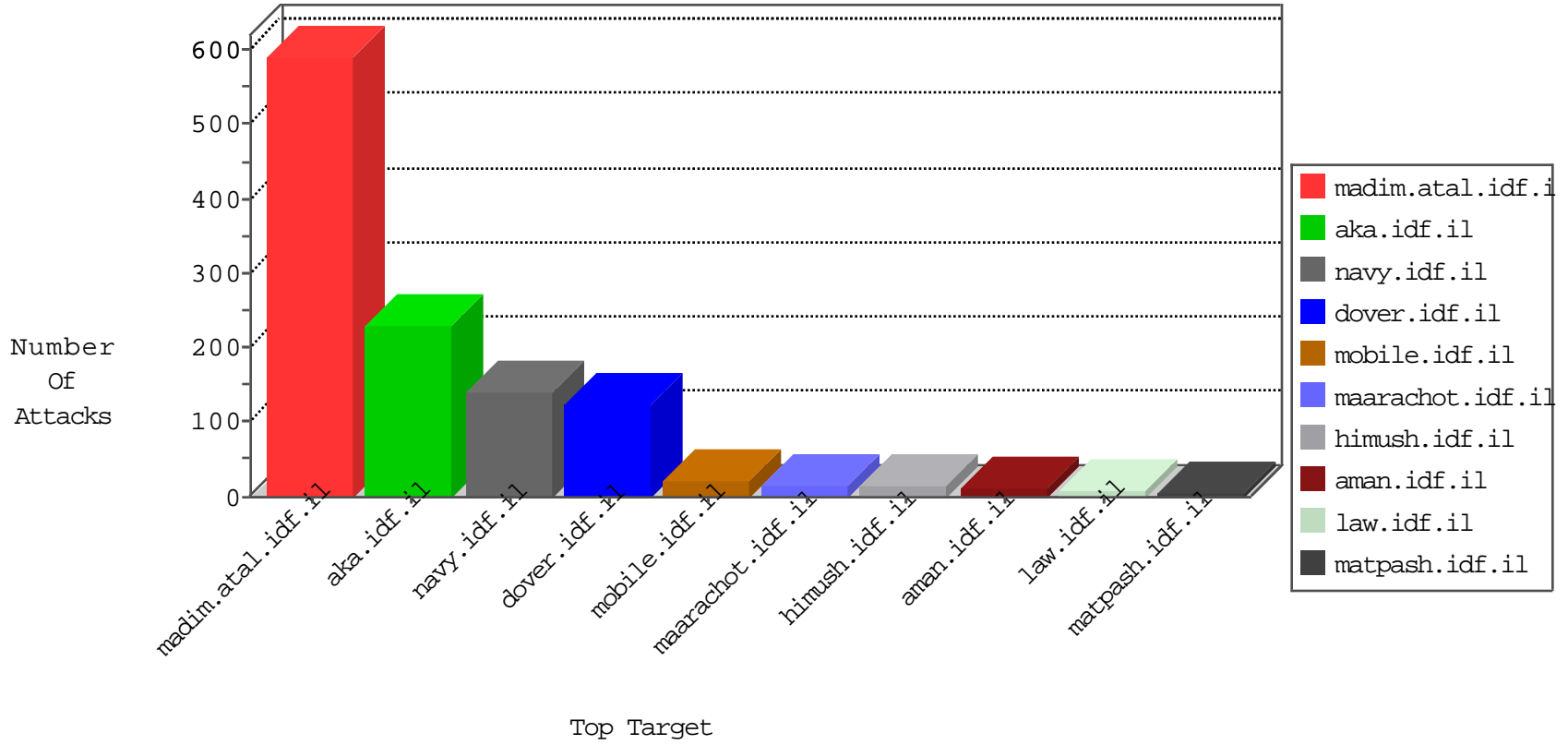


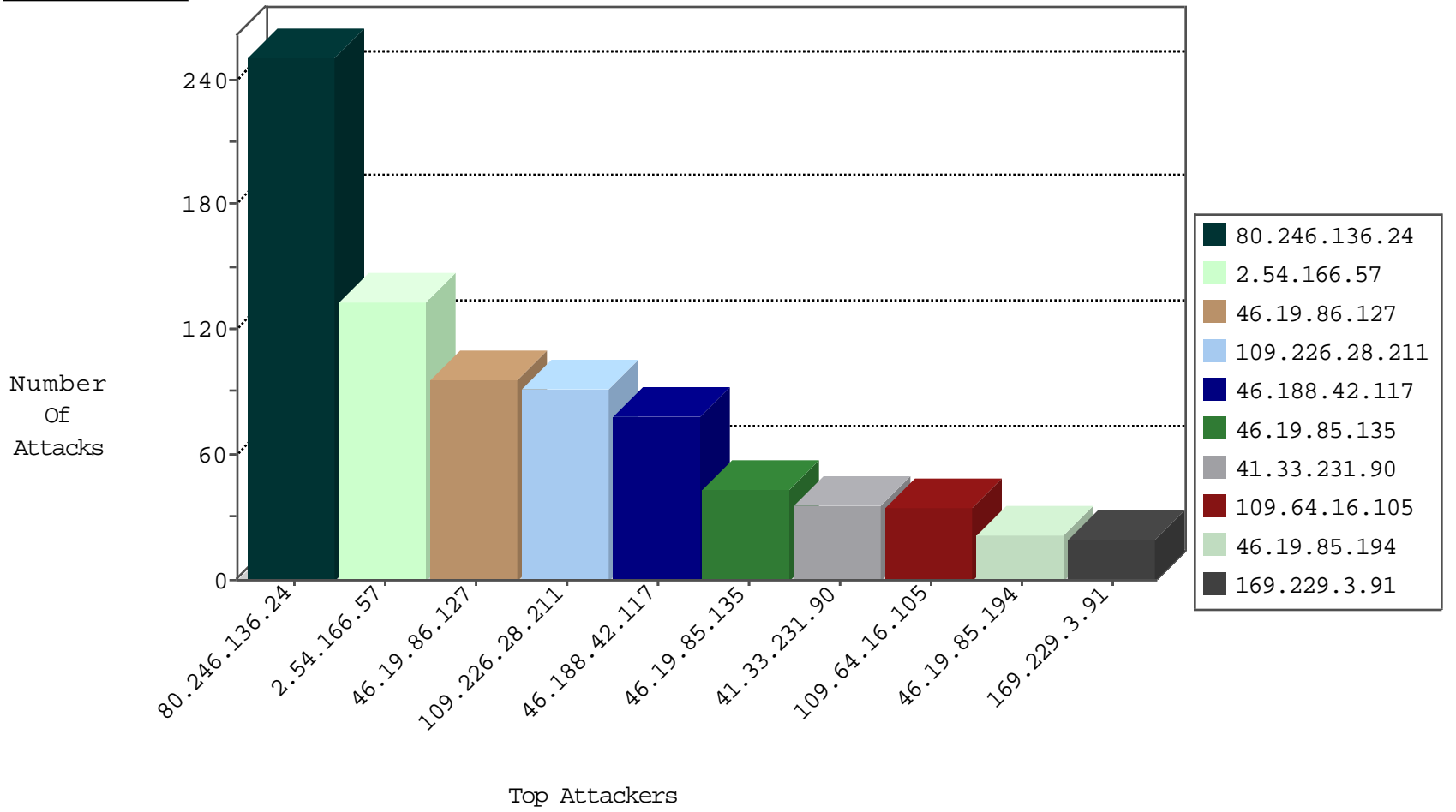
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.151.244.102	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	3
46.188.42.117	Russian Federation	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	2
46.188.42.117	Russian Federation	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
113.108.189.63	China	147.237.77.216	dover.idf.il	block-sp-trafl	drop	1
41.206.63.131	Kenya	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	1
23.239.64.15	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
41.206.63.133	Kenya	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	1
74.82.47.5	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
41.206.63.130	Kenya	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
196.200.16.200	Kenya	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	1
89.248.160.138	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
41.206.63.130	Kenya	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.239.205.207	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	4
213.239.205.207	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
213.239.205.207	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
213.239.205.207	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
69.197.177.26	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.136.24	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	12
195.34.150.18	147.237.77.216	Austria	doover.idf.il	Tehila - Perl LWP with fake user agent	4
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
180.139.164.158	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
122.52.55.208	147.237.76.30	Philippines	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
59.45.79.117	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
223.71.251.11	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
138.122.9.36	147.237.76.30		himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.188.42.117	Russian Federation	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	73
109.64.16.105	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
46.19.85.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.242.28.16	Russian Federation	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	18
79.180.39.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
84.228.26.63	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
197.41.175.99	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
79.182.212.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.190.129	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.194	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.194	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
213.57.140.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
5.102.195.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
5.102.254.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
89.139.181.125	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
185.99.32.3		147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
185.99.32.3		147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.102.170.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
149.78.247.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.132.0	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.213.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.140.216	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
5.22.135.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.183.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.177.25.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.105.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.184.214	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
37.142.68.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.199.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.221.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
81.218.177.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.226.28.211	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.65.10.225	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.116	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.13.119	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.30.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	239
2.54.166.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	133
46.19.86.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
109.226.28.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
46.19.86.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
37.142.160.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
89.139.181.125	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	5
171.249.247.112	Vietnam	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.86.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.226.28.211	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	2
169.229.3.91	United States	147.237.76.30	himush.idf.il	Illegal Byte Code Character in Header Name	Block	1
66.249.66.23	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
109.67.217.208	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 109.67.217.208 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
5.22.135.116	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
93.173.169.170	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
66.249.69.41	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
109.253.210.181	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.67.217.208	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
185.89.217.234		147.237.76.86	navy.idf.il	URL is Above Root Directory www.navy.idf.il/./images/shared/home.png	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Malformed HTTP Header Line 1	Block	1
66.249.66.33	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 66.249.66.33	Block	1
5.29.4.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/	Block	1
109.67.217.208	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
99.32.153.153	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.69.49	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/7/108227.pdf	Block	1
176.13.17.102	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
113.76.90.154	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
109.67.217.208	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method = 'Pöê[[#18]]óðne<[[#18]]~Sb,>ý Áíæú[[#30]]³•[[#28]]p"2[[#3]]Qj,\$sS éE7iCÝÍ^,T> š•B°Á. [[#6]] [[#29]]šsjt[[#16]] [[#18]]•²;fþ	Block	1
188.120.148.104	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
84.111.36.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.66.127	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/sip_storage/files/8/638.pds	Block	1
109.67.217.208	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method = 'Pöê[[#18]]óðne<[[#18]]~Sb,>ý Áíæú[[#30]]³•[[#28]]p"2[[#3]]Qj,\$sS éE7iCÝÍ^,T> š•B°Á. [[#6]] [[#29]]šsjt[[#16]] [[#18]]•²;fþ	Block	1
109.67.217.208	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
66.249.78.158	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
176.228.179.220	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mainsachar	Block	1
138.36.0.3		147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/index.php	Block	1
46.120.156.245	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
109.67.217.208	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version [[#5]]Óð␣({?j~éYKÓŽPž#S(BkçdŪBĪ•ßç=:`#ðJÑÄ, [[#31]]Ö•••ēÑ[[#6]]j@•ö~zS\$[[#2]]pF[[#26]]ç[[#23]]";,UŌÆz₂5ŸŪ ñ[[#27]]6&šŌ ♂^†ŌĪ•ŽŪš*t~ñùPŌŌt	Block	1
212.76.11.242	Kazakstan	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
87.69.181.81	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Malformed URL from 169.229.3.91	Block	1
66.249.66.133	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/usercontrols/headerupper/	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
109.67.217.208	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
79.180.211.120	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
184.105.247.195	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Abnormally Long Request method	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
109.67.217.208	Israel	147.237.72.166	aka.idf.il	Malformed URL *^š	Block	1