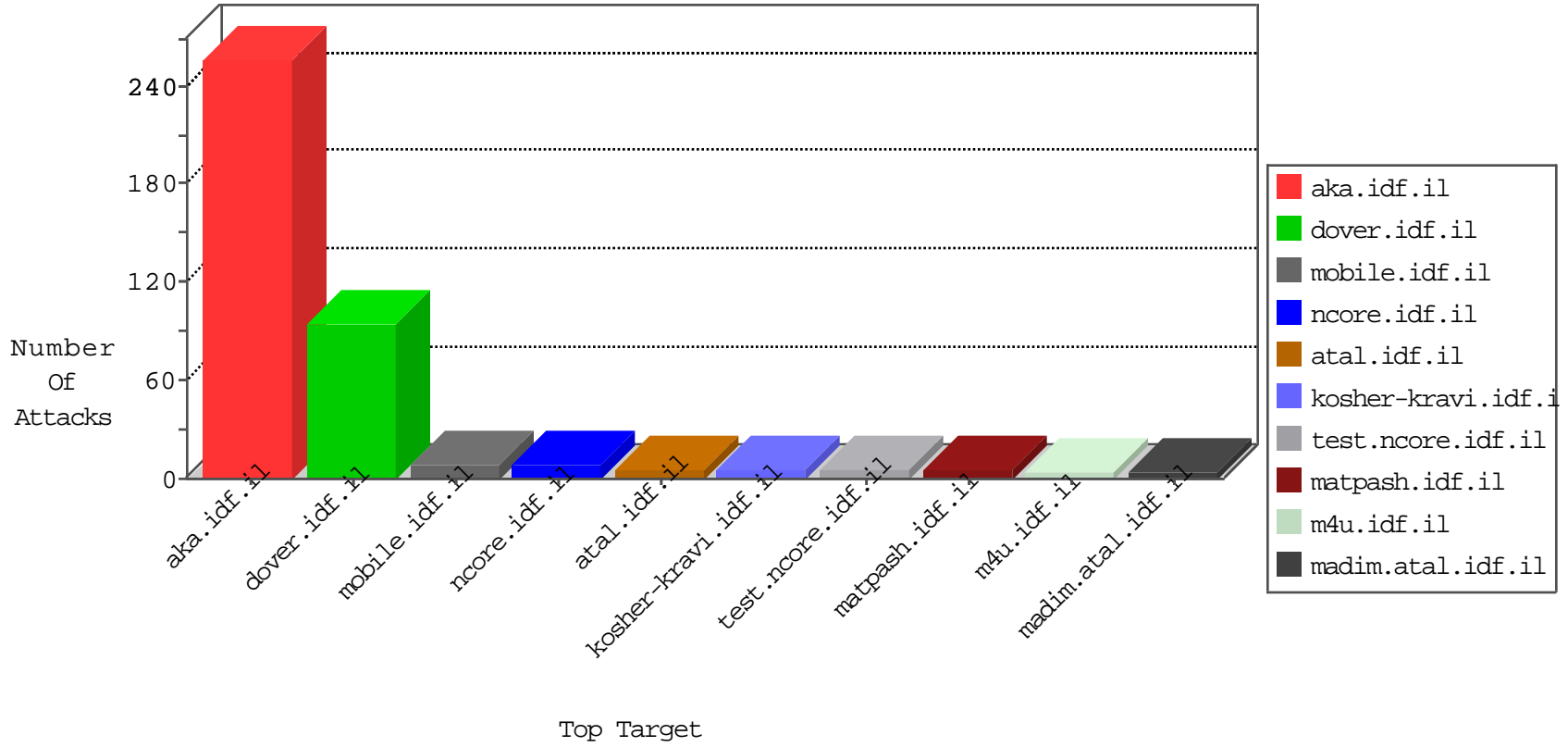


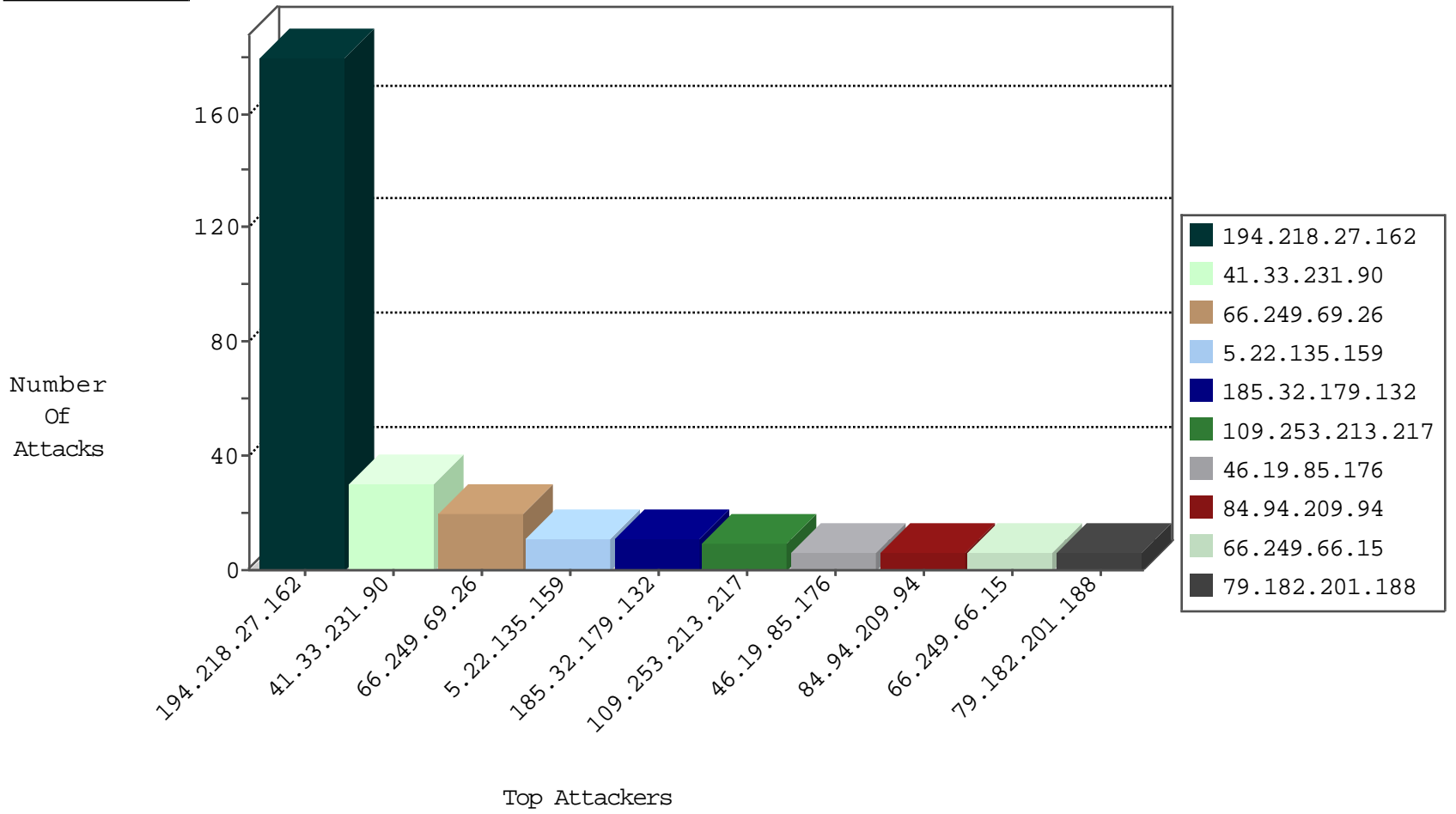
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
217.26.171.188	Moldova, Republic of	147.237.76.176	test.ncore.idf.il	I4 Source or Dest Port Zero	drop	4
103.206.22.24		147.237.0.200	m4u.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
198.23.141.210	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.72	United States	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.212	United States	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
74.82.47.18	United States	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1
198.84.107.122	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.112	United States	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
185.56.28.67	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.116	United States	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
108.4.125.66	United States	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	1
217.26.171.188	Moldova, Republic of	147.237.77.176	matpash.idf.il	I4 Source or Dest Port Zero	drop	1
184.105.139.120	United States	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	doover.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
136.243.103.156	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
198.20.69.74	United States	147.237.76.177	ncore.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

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	4
66.249.69.26	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
173.230.169.99	147.237.76.177	Canada	noore.idf.il	ET SCAN NMAP -f -sS	1
203.197.205.118	147.237.77.227	India	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
115.85.192.40	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.77.19		law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.162	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.97.106.161	147.237.76.200	China	eitan.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.97.106.37	147.237.77.235	China	sviva.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.97.106.37	147.237.72.167	China	ishurim.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.97.106.36	147.237.77.176	China	matpash.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
173.230.169.99	147.237.76.177	Canada	noore.idf.il	ET SCAN NMAP -sS window 2048	1
203.197.205.118	147.237.77.227	India	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
115.85.192.40	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.76.177	United States	noore.idf.il	ET DROP Dshield Block Listed Source	1
88.249.106.23	147.237.76.39	Turkey	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
185.59.31.137	147.237.76.177	Turkey	noore.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.162	147.237.0.15	China	kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.97.106.161	147.237.8.46	China	e.chinuch.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.97.106.37	147.237.76.31	China	nakchal.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.97.106.36	147.237.77.243	China	mobile.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
173.230.169.99	147.237.76.177	Canada	noore.idf.il	ET SCAN NMAP -sS window 3072	1

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	118
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	59
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
109.253.213.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.22.135.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.94.209.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.201.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.15	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.32.179.132	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
5.22.135.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.32.179.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.67.55.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.246.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.136.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.133.160	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.54.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.206.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.88.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.209.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.32.179.132	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
68.46.9.211	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
31.210.186.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.9.131.69	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
74.82.47.47	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.104	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.162	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
218.22.211.69	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.74	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.125.71.117	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
74.82.47.47	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.111	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.163	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
73.222.120.222	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.88	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
138.36.0.3		147.237.0.33	idf.il	drop		drop	1
106.38.241.106	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
216.218.206.82	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.200	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
146.185.239.102	Russian Federation	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.36	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.88	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
138.36.0.3		147.237.0.200	m4u.idf.il	drop		drop	1
106.38.241.106	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	18
46.19.85.71	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
108.235.81.95	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	2
40.77.167.23	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in aka.idf.il/ishurim/cityofficers/	None	1
180.97.106.162	China	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
146.50.79.106	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1785-he/dover.aspx	Block	1
66.249.64.101	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/894-he/nakhal.aspx	Block	1
180.97.106.37	China	147.237.76.31	nakchal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
95.153.129.178	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
66.249.69.32	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
40.77.167.23	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx	None	1
149.88.39.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
74.82.47.3	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
66.249.64.180	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/giyus/general.aspx	Block	1
180.97.106.37	China	147.237.77.235	sviva.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
96.230.113.184	United States	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.87	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
40.77.167.24	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-18630-he/dover.aspx f', - f eš , ÿ f © ½ , š e f ' š , ÿ f "½ , š e f ' , - f eš , ÿ f eš , ½,	Block	1
180.97.106.36	China	147.237.77.176	matpash.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
74.82.47.4	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
66.249.66.33	United States	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
180.97.106.161	China	147.237.76.200	eitan.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.78.94	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
40.77.167.86	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
180.97.106.36	China	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.176.54.14	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
66.249.66.129	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/sitemap/sitemap.aspx	Block	1
37.142.64.93	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar	Block	1
180.97.106.162	China	147.237.0.15	kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.65.88.120	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
68.46.9.211	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
180.97.106.37	China	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.176.54.14	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.176.54.14	Block	1