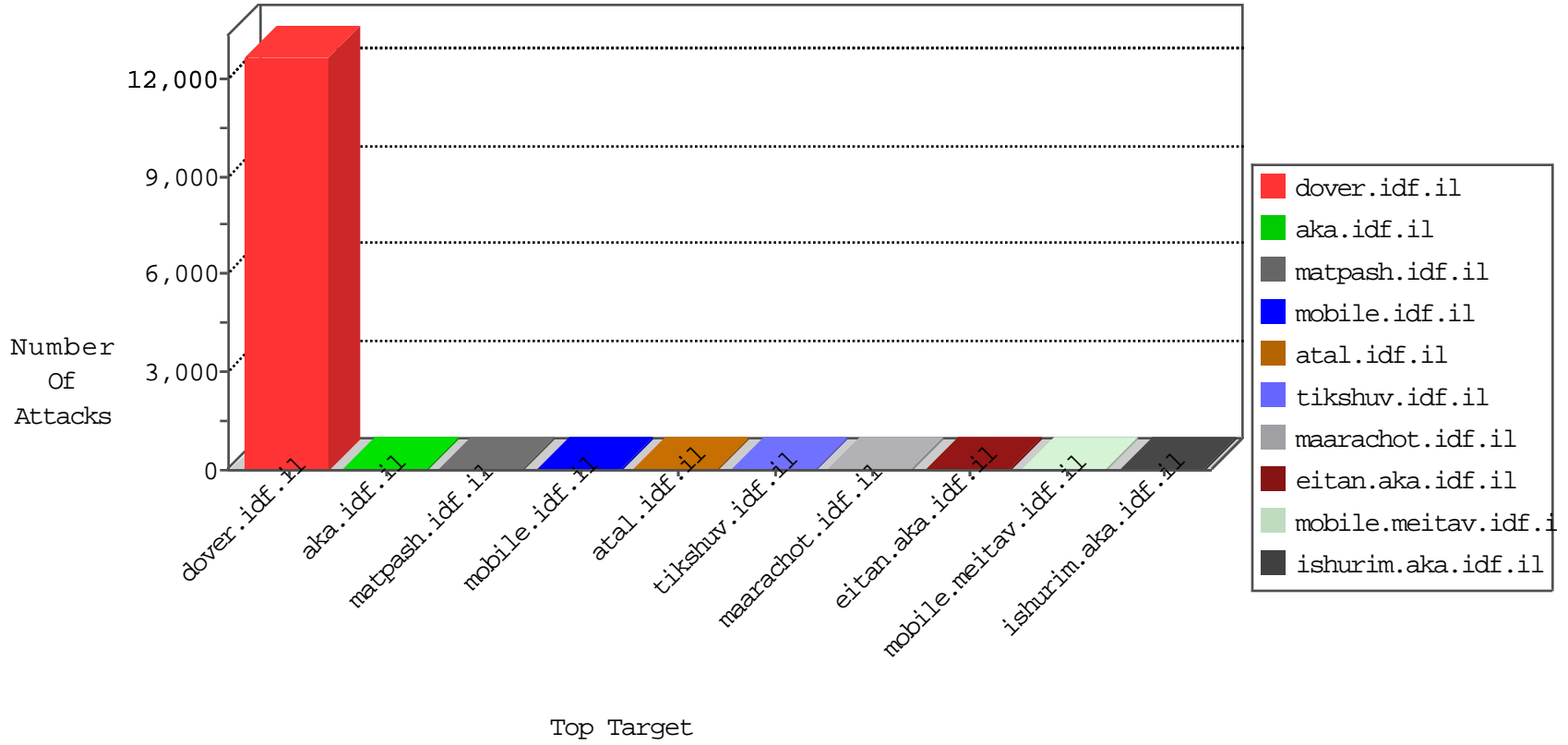


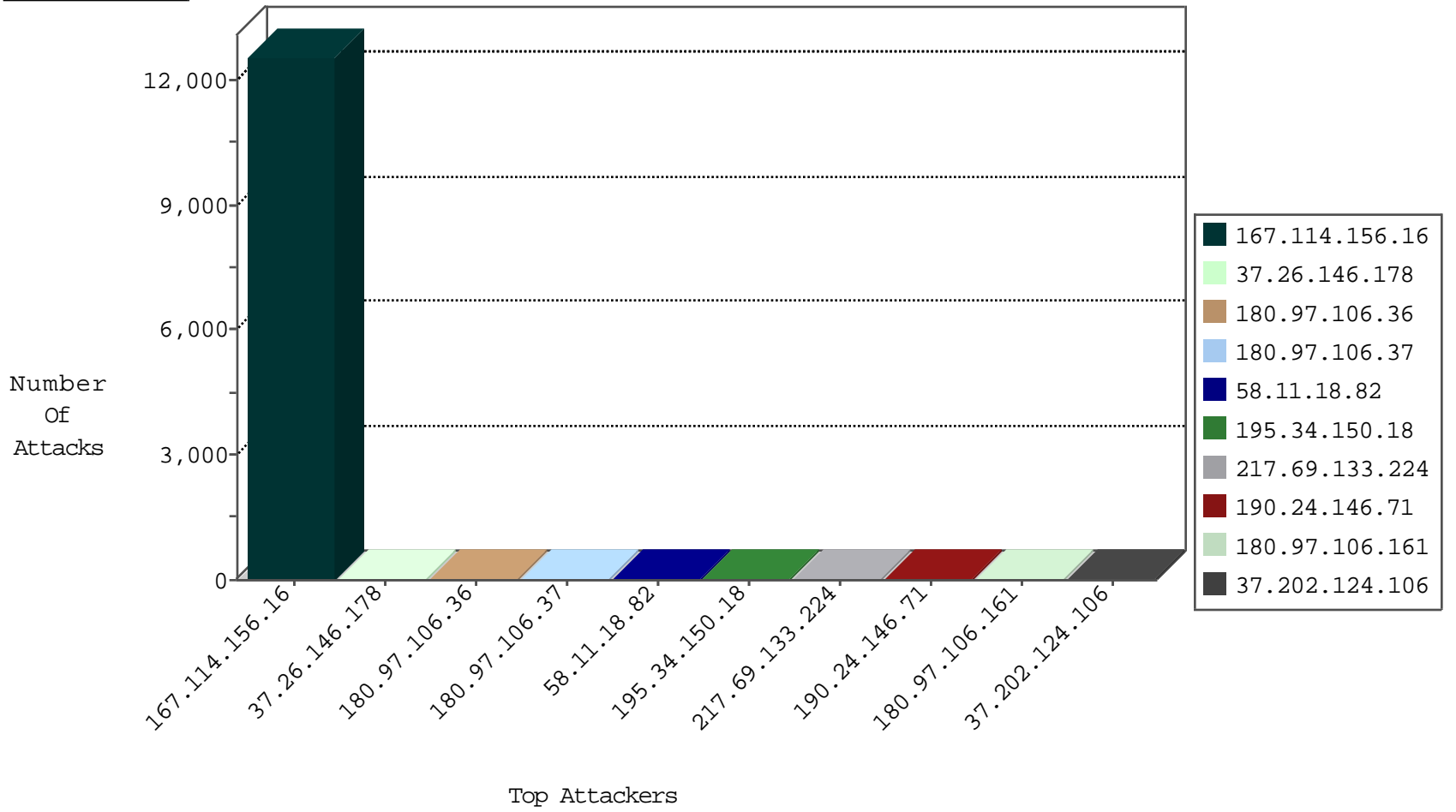
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2078
37.26.146.178	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
66.249.65.238	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
49.143.200.94	Korea, Republic of	147.237.0.200	m4u.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
185.130.5.224		147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
202.116.234.16	China	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
222.75.167.2	147.237.77.216	China	dover.idf.il	GPL SCAN nmap TCP	2
66.249.73.206	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
5.39.222.253	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.77.226	China	www.chamatz.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.97.106.37	147.237.76.38	China	e.e.meitav.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.97.106.37	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
180.97.106.36	147.237.77.234	China	halag.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.97.106.36	147.237.77.179	China	e.mazi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.97.106.162	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
180.97.106.36	147.237.76.39	China	mobile.meitav.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.97.106.162	147.237.0.16	China	my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
104.156.251.148	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.161	147.237.76.177	China	noore.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.97.106.161	147.237.0.17	China	m.my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.97.106.37	147.237.77.216	China	dover.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	147.237.77.235	China	sviva.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
199.191.56.188	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
180.97.106.36	147.237.77.233	China	atal.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
189.218.62.98	147.237.8.14	Mexico	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	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
180.97.106.162	147.237.76.30	China	himush.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
121.224.156.159	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
180.97.106.161	147.237.77.243	China	mobile.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
67.231.20.97	147.237.76.147	Canada	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.161	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9678
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop		drop	1534
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1250
58.11.18.82	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
217.69.133.224	Russian Federation	147.237.72.166	aka.idf.il	drop	SAM rule	drop	8
37.202.124.106	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
109.66.120.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
50.130.160.114	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
194.90.89.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
217.69.133.223	Russian Federation	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
37.46.39.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
107.170.129.218	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	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
94.142.52.154	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
2.54.159.152	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.181.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
217.15.117.118	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
89.145.95.42	United Kingdom	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.69.30	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.28	United Kingdom	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
67.85.30.178	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
199.30.25.140	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.26.146.178	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
104.243.32.242		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.76.148	ggcenter.aka.idf.il	drop		drop	2
108.26.197.220	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.172.193.32	Hungary	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
216.218.206.123	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.102	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
222.75.167.2	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
182.74.243.246	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
217.15.117.118	United Kingdom	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
95.181.217.245	Russian Federation	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
222.75.167.2	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.8	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
182.74.243.246	India	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
5.22.135.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
111.113.13.98	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.246.139.40	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
192.0.112.18	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.26.149.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
75.82.52.189	United States	147.237.77.216	dover.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
104.243.32.242		147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 104.243.32.242	Block	3
193.201.224.8	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 193.201.224.8	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
193.201.224.8	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
66.249.64.17	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/about/memorial	Block	1
180.97.106.37	China	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
173.180.255.19	Canada	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
84.228.149.134	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
180.97.106.161	China	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
2.54.139.215	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
180.97.106.36	China	147.237.77.233	atal.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/pdficon.gif	Block	1
66.249.65.17	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/8/109608.pdf	Block	1
180.97.106.37	China	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
173.180.255.19	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
217.69.133.225	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.68.157.253	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
180.97.106.162	China	147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.69.38	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	1
31.13.113.89	Ireland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://twitter.com/	Block	1
180.97.106.36	China	147.237.77.234	halag.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
180.97.106.37	China	147.237.77.226	www.chamatz.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.65.21	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/2/112562.pdf	Block	1
176.10.104.243	Switzerland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
217.132.28.209	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://twitter.com/	Block	1
180.97.106.162	China	147.237.76.30	himush.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.73.129	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list7.htm	Block	1
38.111.147.84	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-9070-he/atal.aspx	Block	1
180.97.106.36	China	147.237.77.235	sviva.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
157.55.39.169	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21744-ar/idfgdover.aspx	Block	1
79.176.155.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
193.201.224.8	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	1
180.97.106.161	China	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.65.25	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 66.249.65.25	Block	1
180.97.106.36	China	147.237.76.39	mobile.meitav.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
222.155.137.99	New Zealand	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
104.243.32.242		147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/general.aspx	Block	1
180.97.106.162	China	147.237.76.200	eitan.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.78.93	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/894-he	Block	1
46.19.85.130	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
180.97.106.37	China	147.237.0.15	kosher-kravi.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
157.55.39.174	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
79.180.168.70	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
180.97.106.161	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.238	Block	1