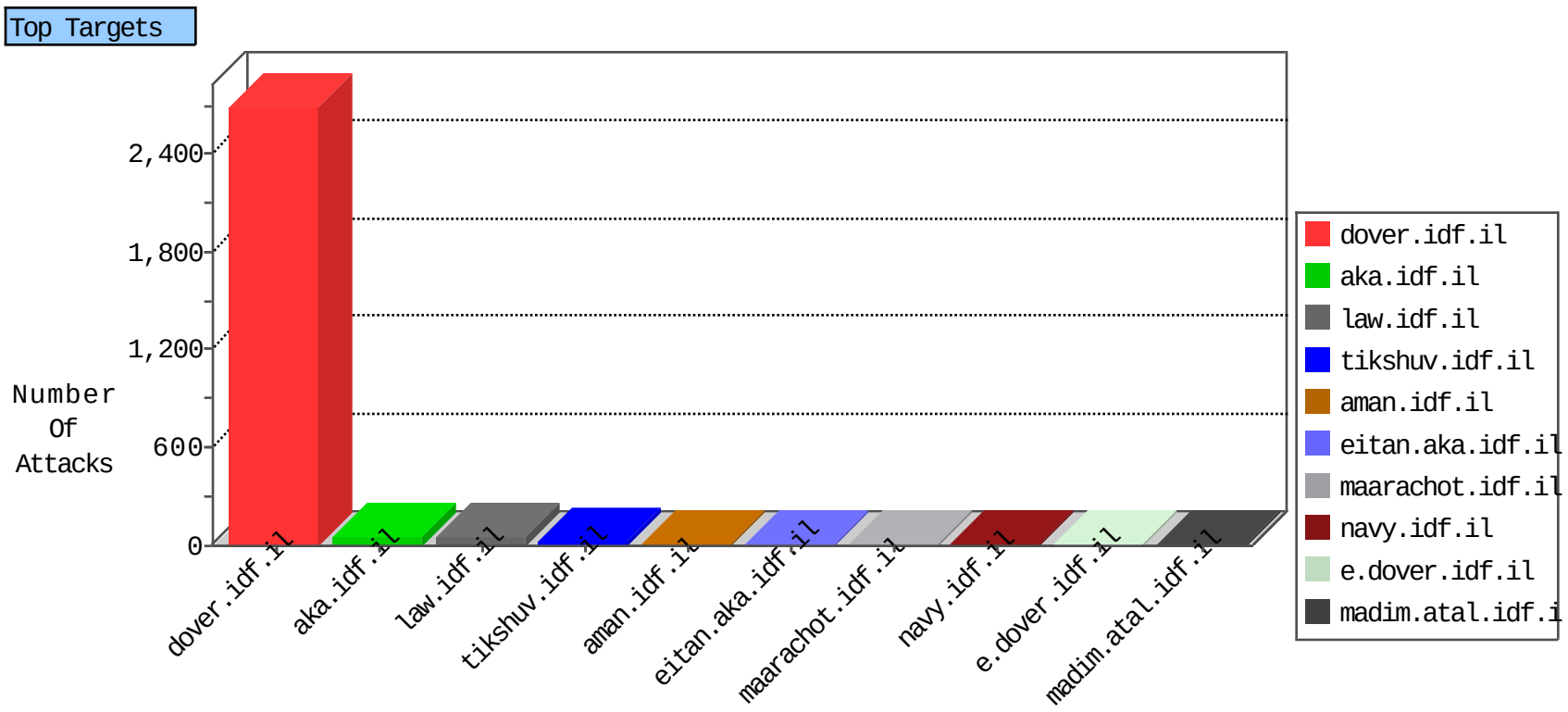
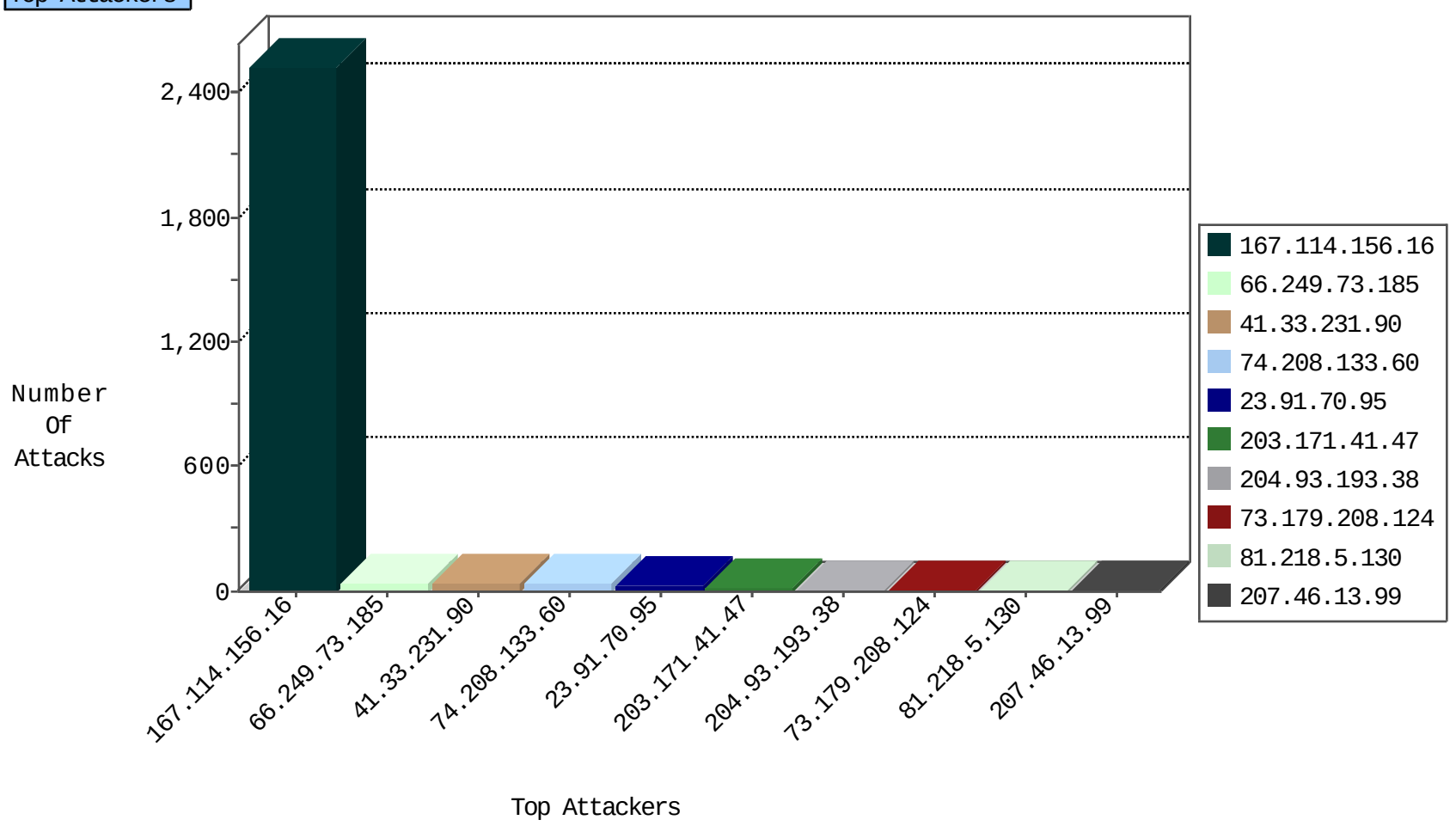
11-26-2015-05:04:00 to 11-26-2015-06:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-26-2015-05:04:00 to 11-26-2015-06:04:00

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	3594
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	82
81.218.5.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
222.186.56.115	China	147.237.76.198	e.yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
198.20.69.98	United States	147.237.76.38	e.e.meitav.idf.i	Block_Udp_All_Nets	drop	1
66.240.192.138	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.151	Netherlands	147.237.76.38	e.e.meitav.idf.i	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	drop	1
80.82.64.198	Netherlands	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
8.17.88.132	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

11-26-2015-05:04:00 to 11-26-2015-06:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
23.91.70.95	United States	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	13
74.208.133.60	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
203.171.41.47	New Zealand	147.237.77.74	law.idf.il	12715: HTTP: Blind SQL Injection in URI	Block	8
23.91.70.95	United States	147.237.0.34	tikshuv.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
74.208.133.60	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
64.186.146.196	United States	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
213.8.145.99	Israel	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
23.91.70.95	United States	147.237.0.34	tikshuv.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	2
64.186.146.196	United States	147.237.77.216	dover.idf.il	3809: HTTP: SQL Injection Evasion SQL Comment Terminator	Block	1

11-26-2015-05:04:00 to 11-26-2015-06:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
74.208.133.60	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
203.171.41.47	147.237.77.74	New Zealand	law.idf.il	SQL Injection - Select From	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.67.232	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
222.186.56.115	147.237.76.177	China	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.160.237.44	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
54.183.246.95	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
222.186.56.115	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.56.115	147.237.76.30	China	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
105.157.74.18	147.237.77.216	Morocco	dover.idf.il	ET SCAN NMAP -sS window 1024	1

11-26-2015-05:04:00 to 11-26-2015-06:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
204.93.193.38	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
73.179.208.124	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
66.249.73.193	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.125.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.99	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
107.107.62.61	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
40.77.167.35	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
157.55.12.72	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
81.63.204.158	Switzerland	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.106.226.219	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
176.106.226.219	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.66.18	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.154.243.114	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.115.95.202	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
207.46.13.49	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
105.157.74.18	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
203.171.41.47	New Zealand	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
105.157.74.18	Morocco	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
64.125.239.227	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.121.183	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
27.130.242.197	Thailand	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
112.74.67.109	China	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
180.153.201.217	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.112.131.241	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
146.185.234.48	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.121.189	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
221.199.217.173	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.116.193.232	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.121.178	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
191.247.230.51	Brazil	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1
74.82.47.22	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.117	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
64.125.239.247	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.121.184	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
112.74.67.109	China	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.200	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
146.185.239.102	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
73.179.208.124	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	1
141.212.122.112	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
64.125.239.76	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.121.178	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
191.247.230.51	Brazil	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
74.82.47.51	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.118	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.186	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
118.238.227.101	Japan	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.204	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.226.172.38	Germany	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	4
2.54.24.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.33.40.198	Romania	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
95.108.158.171	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
83.130.115.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
66.76.174.2	United States	147.237.72.156	aman.idf.il	Multiple signatures from 66.76.174.2	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
141.212.122.112	United States	147.237.77.226	www.chamatz.aka.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
5.255.253.150	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	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
108.92.148.120	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/	Block	1
73.179.208.124	United States	147.237.72.166	aka.idf.il	Multiple signatures from 73.179.208.124	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.65.1	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/894-he	Block	1
146.185.234.48	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.232	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
27.130.242.197	Thailand	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
204.93.193.38	United States	147.237.72.166	aka.idf.il	Distributed MSSQL Data Retrieval with Implicit Conversion Errors(+)	None	1
118.238.227.101	Japan	147.237.72.156	aman.idf.il	Distributed MSSQL Data Retrieval with Implicit Conversion Errors(+)	None	1
66.249.65.101	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
157.55.39.169	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
27.130.242.197	Thailand	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
204.93.193.38	United States	147.237.72.166	aka.idf.il	Multiple signatures from 204.93.193.38	Block	1
118.238.227.101	Japan	147.237.72.156	aman.idf.il	Multiple signatures from 118.238.227.101	Block	1
88.198.26.46	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 88.198.26.46	Block	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
180.153.180.190	China	147.237.0.34	tikshuv.idf.il	URL is Above Root Directory www.tikshuv.idf.il/../shared/clientscripts/ui/ui.datepicker.js	Block	1
66.249.67.243	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1
66.76.174.2	United States	147.237.72.156	aman.idf.il	Distributed MSSQL Data Retrieval with Implicit Conversion Errors(+)	None	1
207.46.13.177	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
141.212.122.112	United States	147.237.77.216	dover.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
88.198.26.46	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/main/	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.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
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
73.179.208.124	United States	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1