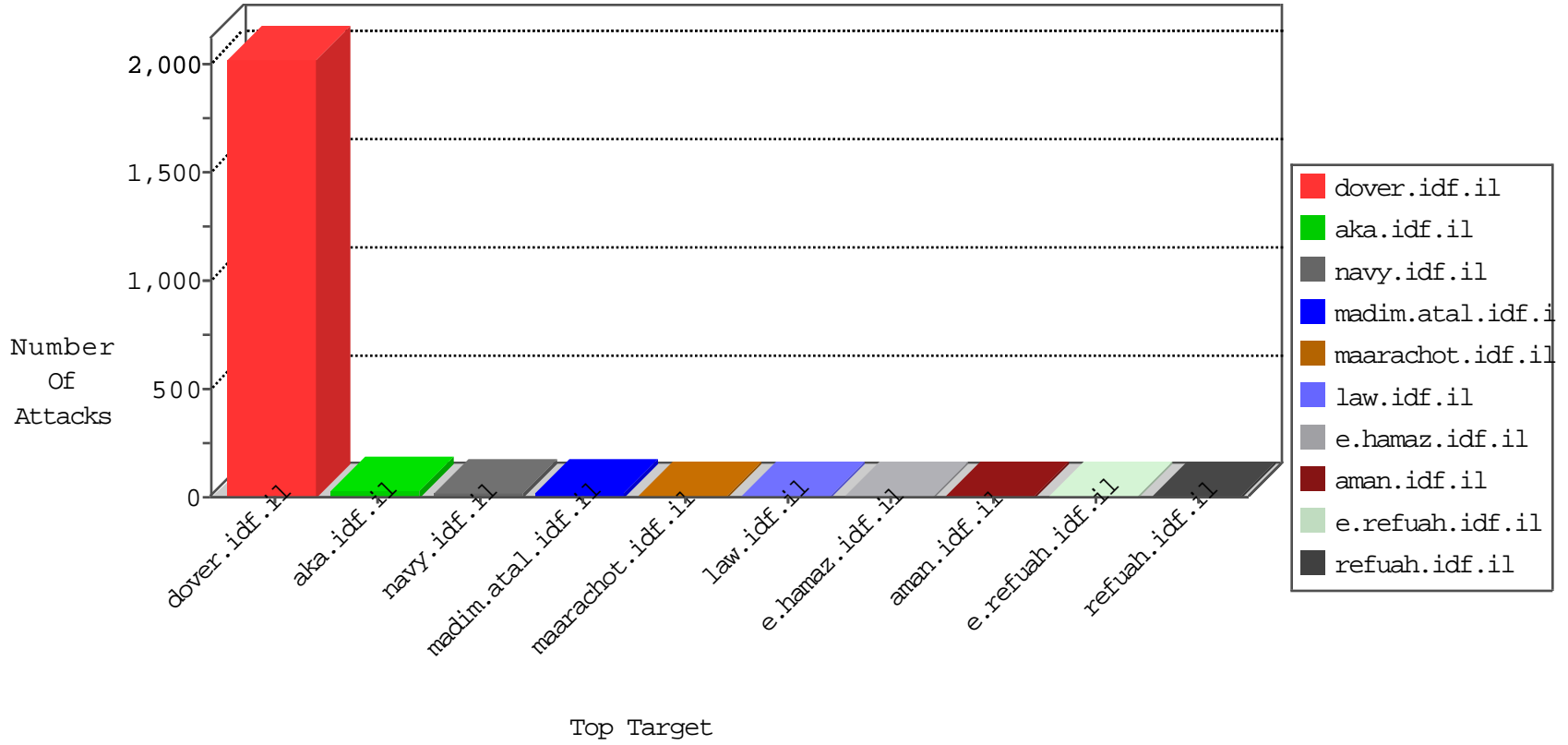


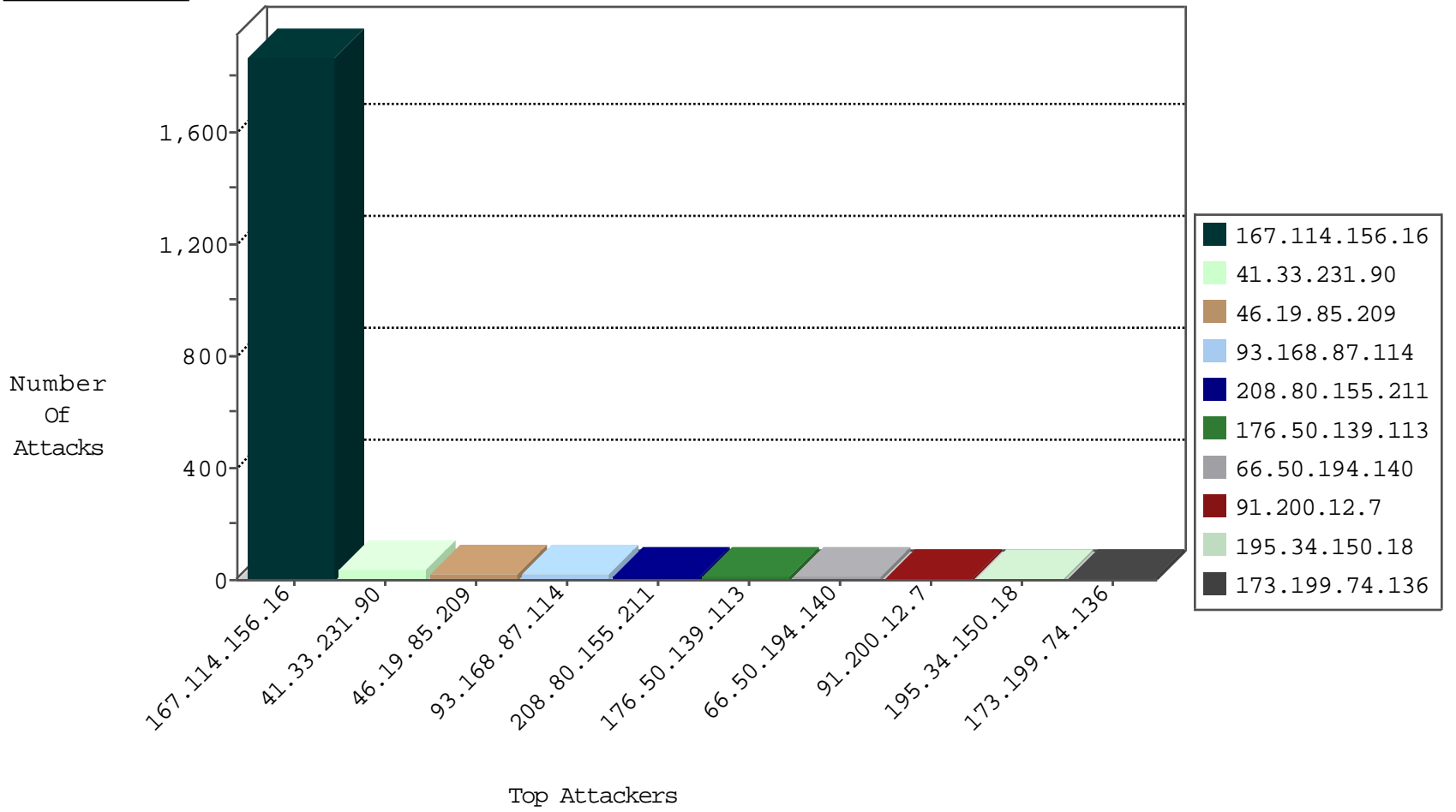
IDF Under Attack Daily Report



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	3168
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1281
204.42.253.2	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	2
65.181.113.88	United States	147.237.76.176	test.ncore.idf.i	Block_Ntp_All_Net	drop	1

01-08-2016-04:04:05 to 01-08-2016-05:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.235.214.119	United States	147.237.77.233	atal.idf.	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	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
176.50.139.113	147.237.77.227	Russian Federation	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
176.50.139.113	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
208.80.155.211	147.237.76.86	United States	navy.idf.il	Tehila - Perl LWP with fake user agent	2
176.50.139.113	147.237.76.177	Russian Federation	ncore.idf.il	ET SCAN Potential SSH Scan	2
208.80.155.211	147.237.72.166	United States	aka.idf.il	Tehila - Perl LWP with fake user agent	2
173.199.74.136	147.237.0.33	United Kingdom	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
176.50.139.113	147.237.76.197	Russian Federation	e.himush.idf.il	ET SCAN Potential SSH Scan	1
99.129.251.54	147.237.77.74	United States	law.idf.il	ET SCAN Potential SSH Scan	1
176.50.139.113	147.237.76.148	Russian Federation	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
176.50.139.113	147.237.72.217	Russian Federation	e.idf.il	ET SCAN Potential SSH Scan	1
176.50.139.113	147.237.8.50	Russian Federation	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.77.61	United States	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.77.227	United Kingdom	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.76.147	United Kingdom	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.8.24	United Kingdom	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
176.50.139.113	147.237.77.170	Russian Federation	maarachot.idf.il	ET SCAN Potential SSH Scan	1
106.75.199.201	147.237.72.156	China	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
99.129.251.54	147.237.77.61	United States	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
176.50.139.113	147.237.76.38	Russian Federation	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
176.50.139.113	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN Potential SSH Scan	1
176.50.139.113	147.237.8.27	Russian Federation	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
176.50.139.113	147.237.0.15	Russian Federation	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
173.199.74.136	147.237.77.74	United Kingdom	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.8.27	United Kingdom	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
93.168.87.114	Romania	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
93.168.87.114	Romania	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
46.19.85.209	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.209	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
93.168.87.114	Romania	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
208.80.155.211	United States	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
82.145.222.84	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
69.136.18.200	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
80.246.136.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.50.194.140	Puerto Rico	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
91.200.12.7	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
66.50.194.140	Puerto Rico	147.237.77.216	dover.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
79.177.49.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.108.94.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
208.80.155.211	United States	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
66.50.194.140	Puerto Rico	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.108.94.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
208.80.155.211	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
78.250.72.87	France	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
141.212.122.100	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
66.50.194.140	Puerto Rico	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.75	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
93.174.93.96	Netherlands	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.123	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
83.166.234.5	Russian Federation	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.104	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
69.125.162.54	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.94	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.70	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
203.127.96.217	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
180.150.185.107	China	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.101	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.81	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.75.199.201	China	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.215	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
149.202.240.85	Germany	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.95	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.74	United States	147.237.8.24	e.lifestyle.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
94.159.169.170	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	5
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
84.111.187.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19122-en/dover.aspx http://startowy.com/dodajlink.html	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.38	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1734	Block	1
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	1
107.178.195.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
78.250.72.87	France	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
208.80.155.224	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/yohalan/main/main.asp	Block	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	WEB MISC Unauthorized File Access	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1540-13036-he/dover.aspx target=	Block	1
188.143.232.11	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.11	Block	1
45.74.19.9		147.237.77.233	atal.idf.il	eMail Hoarding	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	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
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
66.249.73.129	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/pratim/pirteykufa	Block	1
109.201.154.243	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
78.250.72.87	France	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
188.143.232.11	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/article.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
46.19.86.49	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.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
66.249.73.147	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list3.htm	Block	1
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xhlllytayltawms5kb2m=&infocenteritem=true	Block	1
109.253.139.32	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
83.166.234.5	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1512-he/refuah.aspx	Block	1
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xhlllytalltawmy5kb2m=&infocenteritem=true	Block	1
66.50.194.140	Puerto Rico	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
106.75.199.201	China	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 68.180.228.175	Block	1
208.80.155.211	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 208.80.155.211	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	1
141.212.122.64	United States	147.237.0.19	madim.atal.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
5.29.207.74	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
83.166.234.5	Russian Federation	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/gallery	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
66.180.193.219	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/main.stm,	Block	1
107.178.195.167	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
208.80.155.211	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/yohalan/main/main.asp	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1