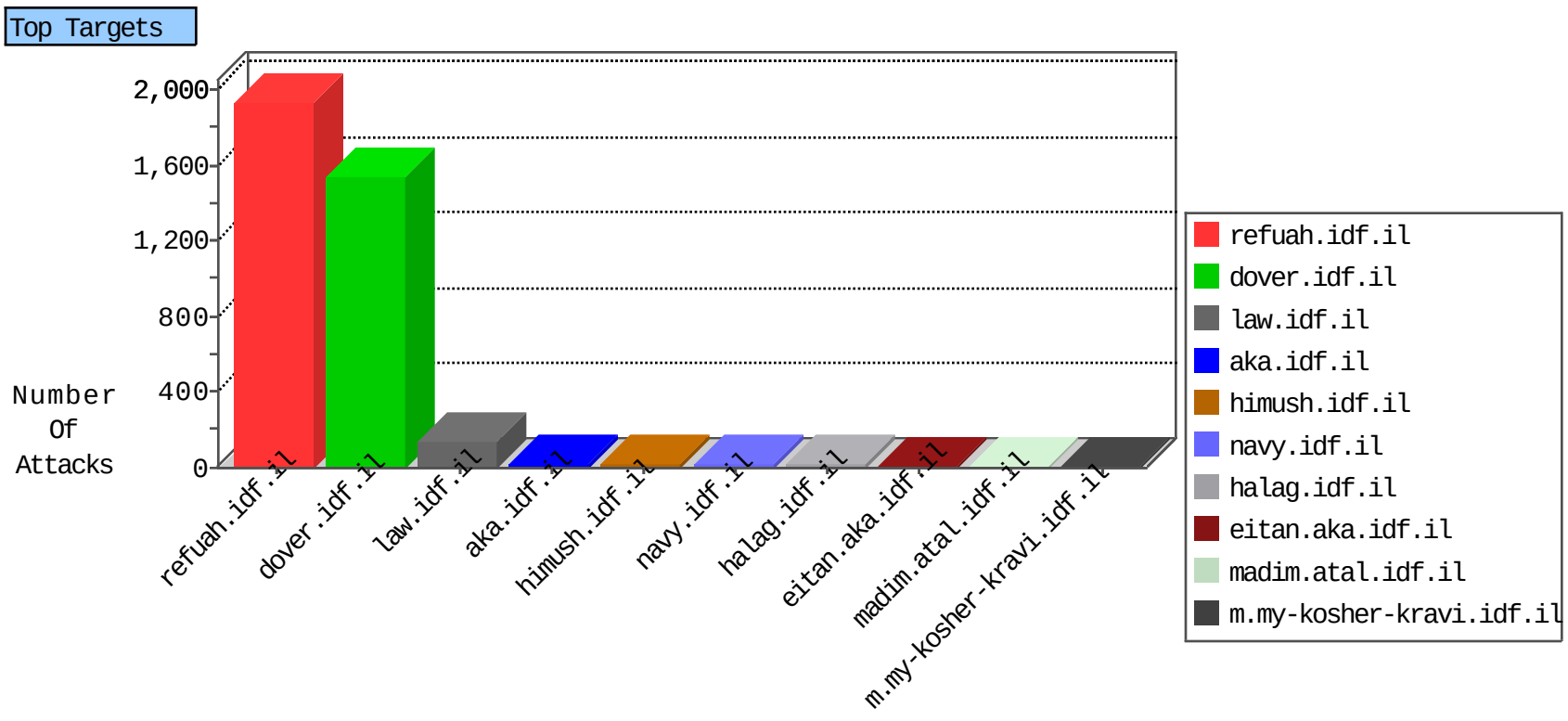
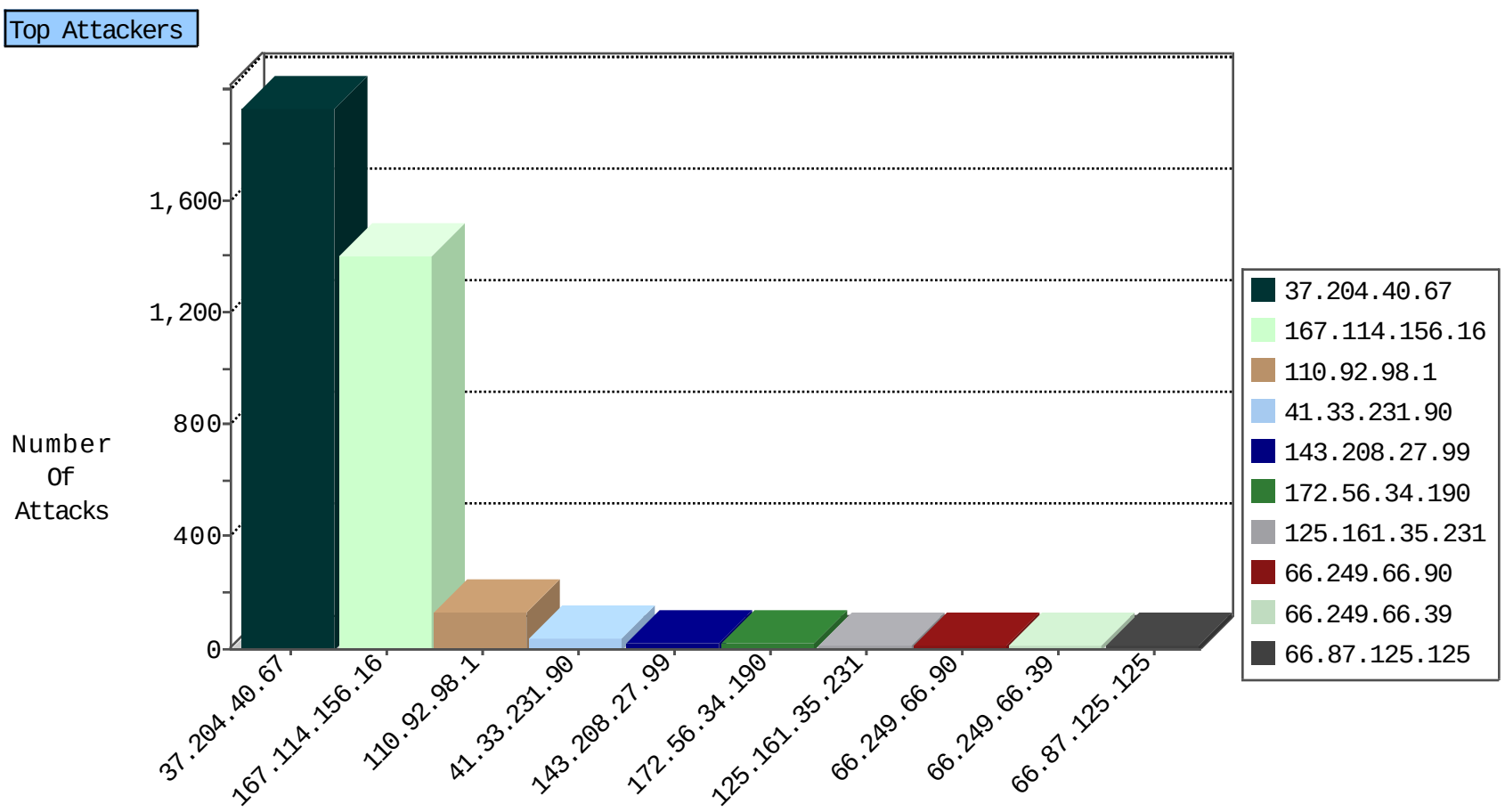
12-15-2015-04:04:06 to 12-15-2015-05:04:06

IDF Under Attack Daily Report



Top Target



Top Attackers

12-15-2015-04:04:06 to 12-15-2015-05:04:06

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	3663
146.185.239.100	Russian Federation	147.237.77.170	maarachot.idf.il	block-sp-traf1	drop	1
185.106.94.126		147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1

12-15-2015-04:04:06 to 12-15-2015-05:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

12-15-2015-04:04:06 to 12-15-2015-05:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.36	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
143.208.27.99	147.237.76.30		himush.idf.il	ET SCAN Potential SSH Scan	2
143.208.27.99	147.237.76.200		eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
143.208.27.99	147.237.8.14		e.orchot.idf.il	ET SCAN Potential SSH Scan	2
143.208.27.99	147.237.76.42		refuah.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.38	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
58.253.96.122	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
143.208.27.99	147.237.8.46		e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
199.191.56.187	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
58.253.96.122	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
143.208.27.99	147.237.8.27		e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
143.208.27.99	147.237.0.200		m4u.idf.il	ET SCAN Potential SSH Scan	1
143.208.27.99	147.237.77.227		e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
143.208.27.99	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
143.208.27.99	147.237.77.212		e.dover.idf.il	ET SCAN Potential SSH Scan	1
137.117.34.247	147.237.76.86	United States	navy.idf.il	ET SCAN Potential SSH Scan	1
137.117.34.247	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
143.208.27.99	147.237.76.196		e.sviva.idf.il	ET SCAN Potential SSH Scan	1
66.249.66.185	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
143.208.27.99	147.237.76.34		yohalan.idf.il	ET SCAN Potential SSH Scan	1
143.208.27.99	147.237.8.50		e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
199.191.56.187	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
58.253.96.122	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
143.208.27.99	147.237.8.45		e.eitan.idf.il	ET SCAN Potential SSH Scan	1
199.191.56.187	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
23.97.172.218	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.7	147.237.72.14	Ukraine	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
143.208.27.99	147.237.0.34		tikshuv.idf.il	ET SCAN Potential SSH Scan	1
143.208.27.99	147.237.77.216		dover.idf.il	ET SCAN Potential SSH Scan	1
137.117.34.247	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
143.208.27.99	147.237.77.178		e.matpash.idf.il	ET SCAN Potential SSH Scan	1
137.117.34.247	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
143.208.27.99	147.237.76.199		e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
137.117.34.247	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

12-15-2015-04:04:06 to 12-15-2015-05:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.204.40.67	Russian Federation	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	1930
110.92.98.1	Singapore	147.237.77.74	law.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	64
110.92.98.1	Singapore	147.237.77.74	law.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	64
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
172.56.34.190	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
125.161.35.231	Indonesia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
66.249.66.16	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
125.39.9.149	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
199.30.25.81	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
166.182.83.94	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
198.90.112.27	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.87.125.125	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
104.196.87.187	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.87.125.125	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
84.95.212.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.87.125.125	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
66.87.125.125	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
125.39.9.149	China	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	2
66.249.66.42	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.204.40.67	Russian Federation	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.64.70	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.26.149.154	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
128.232.110.28	United Kingdom	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.116.177.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.66.95	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
141.212.121.179	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.216	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.60	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.121.189	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.78	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
137.116.71.170	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.116.177.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
180.76.15.20	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.26	United States	147.237.77.61	e.cogat.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.68	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.180	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.102.204.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.223	United States	147.237.0.35	akaws.idf.il	drop		drop	1
153.92.127.143	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.64	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
139.196.104.39	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

12-15-2015-04:04:06 to 12-15-2015-05:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
40.77.167.44	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	4
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	2
66.249.66.77	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.61	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation PageNum in www.tikshuv.idf.il/901-he/tikshuv.aspx	Block	2
208.115.113.93	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
176.12.141.71	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Double URL Encoding - parameter: ReturnUrl in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	1
104.131.161.59	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
66.249.73.225	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/m/	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
66.249.66.65	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
141.212.122.64	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
5.22.129.144	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	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
66.249.66.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/4/60984.pdf	Block	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-18848-he/kkkkkkk=6de3a06ekkkkkkk_6de3a06e	Block	1
66.249.79.106	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1407-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
141.212.122.64	United States	147.237.72.167	ishurim.aka.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
31.13.110.101	Ireland	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
74.6.254.127	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily_statistics/english/1.doc.	Block	1
66.249.66.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
216.218.206.66	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
66.249.66.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
180.76.15.19	China	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	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
66.249.79.108	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1408-he/atal.aspx	Block	1
208.115.111.74	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.80	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
84.229.158.217	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.191	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
180.76.15.146	China	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	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
66.249.66.83	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.70	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/983-en/eitan.aspx	None	1
167.114.0.27	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
104.131.5.73	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.m.my-kosher-kravi.idf.il/	Block	1
66.249.73.225	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 66.249.73.225	Block	1
184.105.247.196	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
125.39.9.149	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../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/1133-ar/dover.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.84	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1

12-15-2015-04:04:06 to 12-15-2015-05:04:06