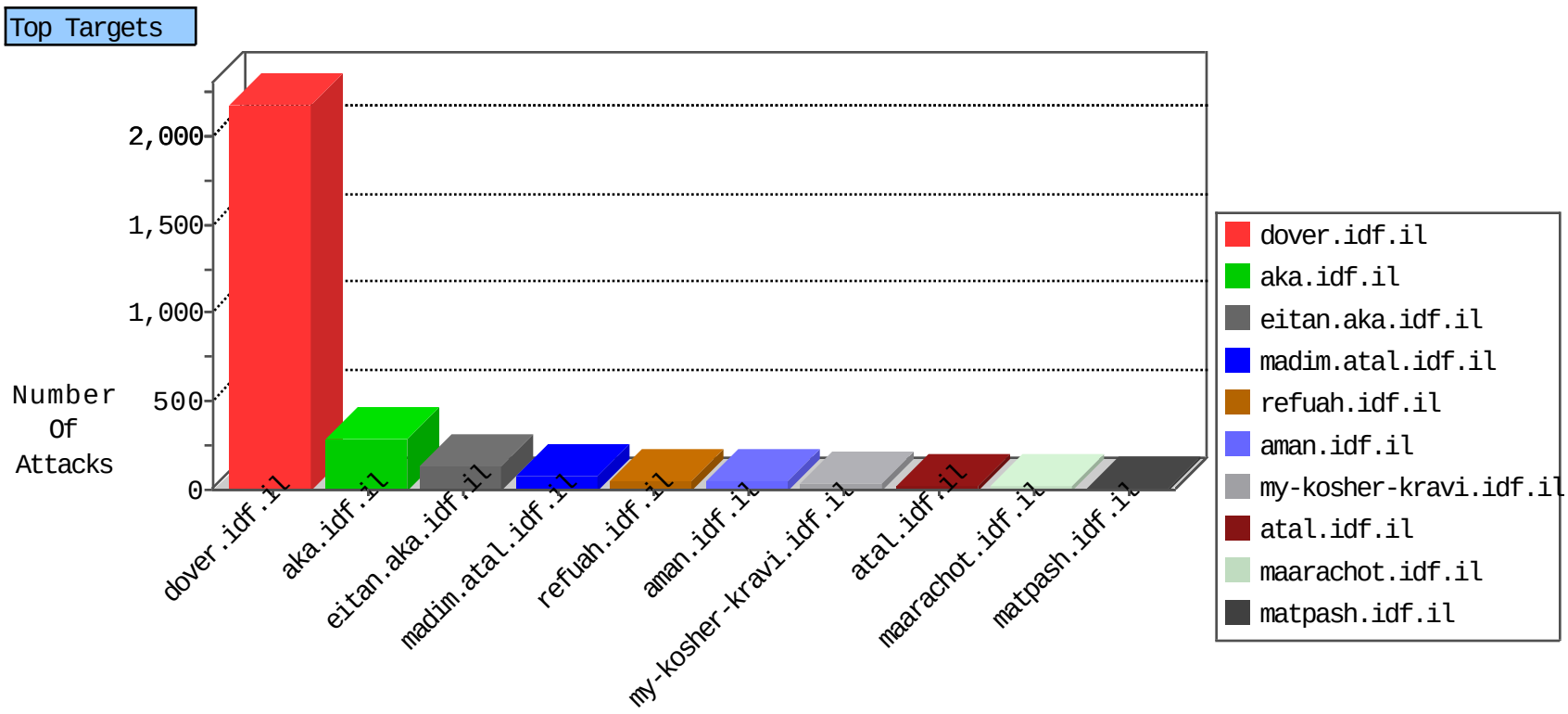
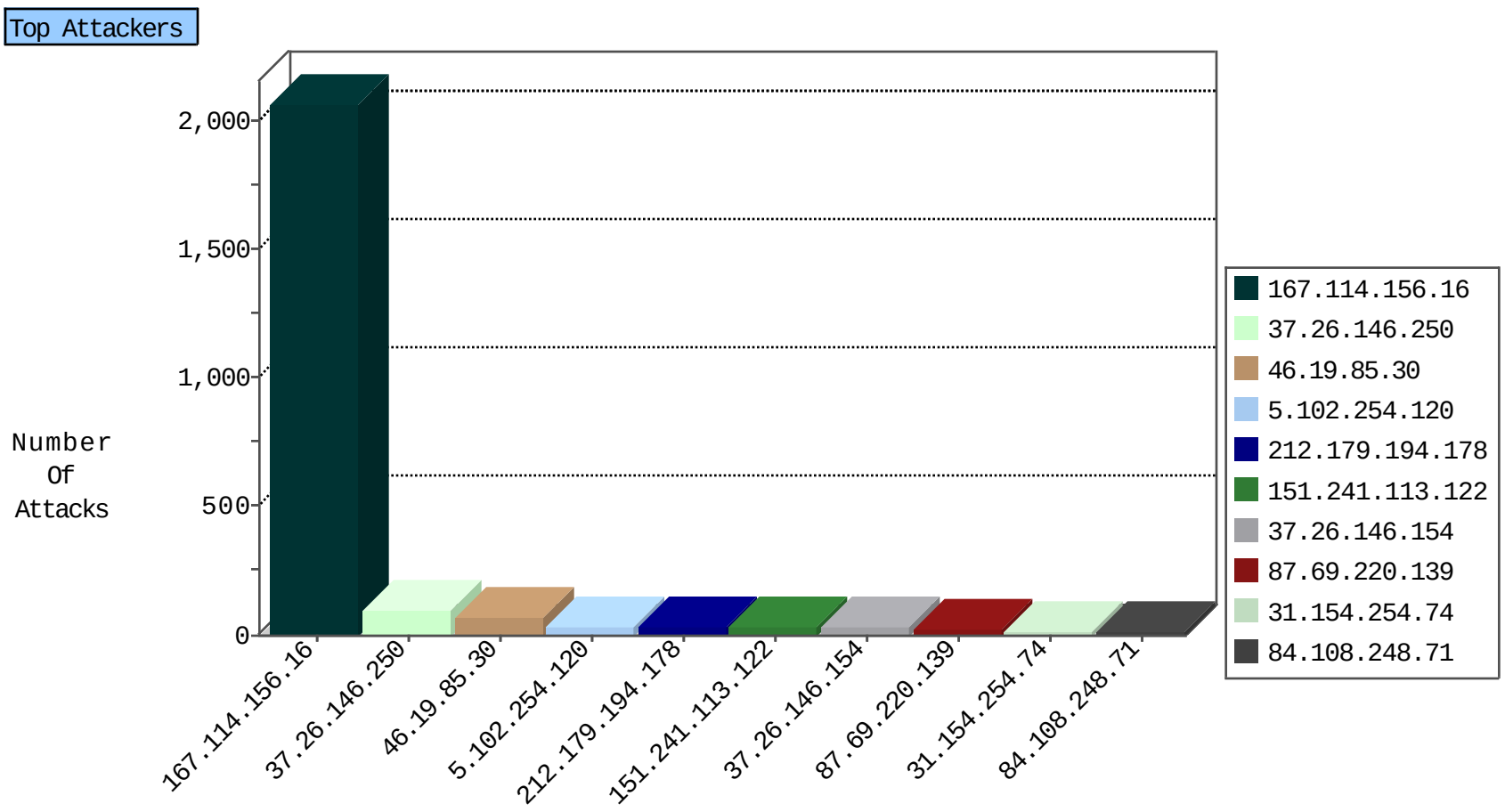
12-05-2015-20:04:02 to 12-05-2015-21:04:02

IDF Under Attack Daily Report





12-05-2015-20:04:02 to 12-05-2015-21:04:02

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	3677
66.249.64.181	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	162
5.189.143.175	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
73.238.33.10	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
5.189.143.175	Germany	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
73.238.33.10	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1

12-05-2015-20:04:02 to 12-05-2015-21:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.121.211.59	France	147.237.77.216	dover.idf.i	C1000106: HTTP: majestic bot	Block	1
94.102.56.143	Netherlands	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
144.76.29.66	Germany	147.237.77.216	dover.idf.i	C1000106: HTTP: majestic bot	Block	1
80.93.90.96	France	147.237.76.86	navy.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

12-05-2015-20:04:02 to 12-05-2015-21:04:02

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
66.249.78.14	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
40.115.58.160	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
180.153.104.125	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 2048	1
138.255.66.227	147.237.8.14		e.orchot.idf.il	ET SCAN Potential SSH Scan	1
138.255.66.227	147.237.0.19		madim.atal.idf.il	ET SCAN Potential SSH Scan	1
122.114.17.100	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
122.114.17.100	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.76.197		e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.224.8	147.237.76.42	Ukraine	refuah.idf.il	SERVER-WEBAPP admin.php access	1
40.115.58.160	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
180.153.104.125	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -f -sS	1
138.255.66.227	147.237.0.34		tikshuv.idf.il	ET SCAN Potential SSH Scan	1
122.114.17.100	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
122.114.17.100	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
69.84.245.76	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1

12-05-2015-20:04:02 to 12-05-2015-21:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
37.26.146.250	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	99
37.26.146.154	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
5.102.254.120	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
87.69.220.139	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
212.179.194.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
212.179.194.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
5.102.254.120	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
46.121.135.51	Israel	147.237.0.16	my-kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
199.30.25.255	United States	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
31.154.254.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
84.108.248.71	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
109.65.118.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.140.160	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.67.186.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
157.55.39.217	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.228.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.154.254.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.65.199.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.183.176.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.179.17.233	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
84.108.248.71	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
213.57.128.185	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
151.241.113.122	Iran, Islamic Republic of	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
109.66.8.4	Israel	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
151.241.113.122	Iran, Islamic Republic of	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.51	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.154.254.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
84.228.184.173	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
151.241.113.122	Iran, Islamic Republic of	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
5.29.209.176	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.181.254.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.17.138.156	Iraq	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
5.29.209.176	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
79.181.254.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.156.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.50.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.166.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.54.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.146.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.137.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.119.49	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
84.108.248.71	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.54.128.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.34.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.198.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.64.38.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

12-05-2015-20:04:02 to 12-05-2015-21:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
84.108.36.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.16.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.179.99.94	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
79.179.99.94	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	3
46.19.85.233	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 46.19.85.233	None	3
193.201.224.8	Ukraine	147.237.76.42	refuah.idf.il	PHP Attempt	Block	2
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	2
109.67.37.201	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
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	2
151.241.113.122	Iran, Islamic Republic of	147.237.72.167	ishurim.aka.idf.il	Multiple Malformed URL from 151.241.113.122	Block	2
176.12.142.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
151.241.113.122	Iran, Islamic Republic of	147.237.72.156	aman.idf.il	Multiple Malformed URL from 151.241.113.122	Block	2
109.66.104.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
193.201.224.8	Ukraine	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 193.201.224.8	Block	2
93.172.170.82	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 93.172.170.82	Block	2
151.241.113.122	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Malformed URL *	Block	1
5.102.254.120	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
94.102.56.143	Netherlands	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.66.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58604&docid=73550	Block	1
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
130.193.50.11	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
87.68.56.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
79.180.48.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.14.81	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 109.66.14.81 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
76.72.161.76	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 76.72.161.76	Block	1
5.255.253.194	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
95.108.158.168	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
5.29.99.241	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
93.172.170.82	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	1
66.249.66.43	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20422-he/idfgdover.aspx	Block	1
151.241.113.122	Iran, Islamic Republic of	147.237.72.166	aka.idf.il	Multiple Malformed URL from 151.241.113.122	Block	1
46.19.86.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.140.141.35	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
79.178.138.178	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1361-10625-he/dover.aspx&sa=u&ved=0ahukewjmjvl_7mtjahxirhqkhy6rbf4qfggrmae&usg=afqjcnf_b016rnmdjafppqlxngfli8du6w	Block	1
185.27.105.141	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
66.249.78.134	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/894-en	Block	1
151.241.113.122	Iran, Islamic Republic of	147.237.77.233	atal.idf.il	Multiple Malformed URL from 151.241.113.122	Block	1
5.102.254.120	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
94.102.56.143	Netherlands	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
141.8.142.2	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
87.69.220.139	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
79.180.126.219	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
193.201.224.8	Ukraine	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-login.php	Block	1
46.19.85.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.14.81	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
76.72.161.76	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
176.13.22.117	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
8.37.71.78	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22976-he/dover.aspx&usg=alkjrhgj9fnltgdbnbl73njc7m0xowv6ag	Block	1

12-05-2015-20:04:02 to 12-05-2015-21:04:02