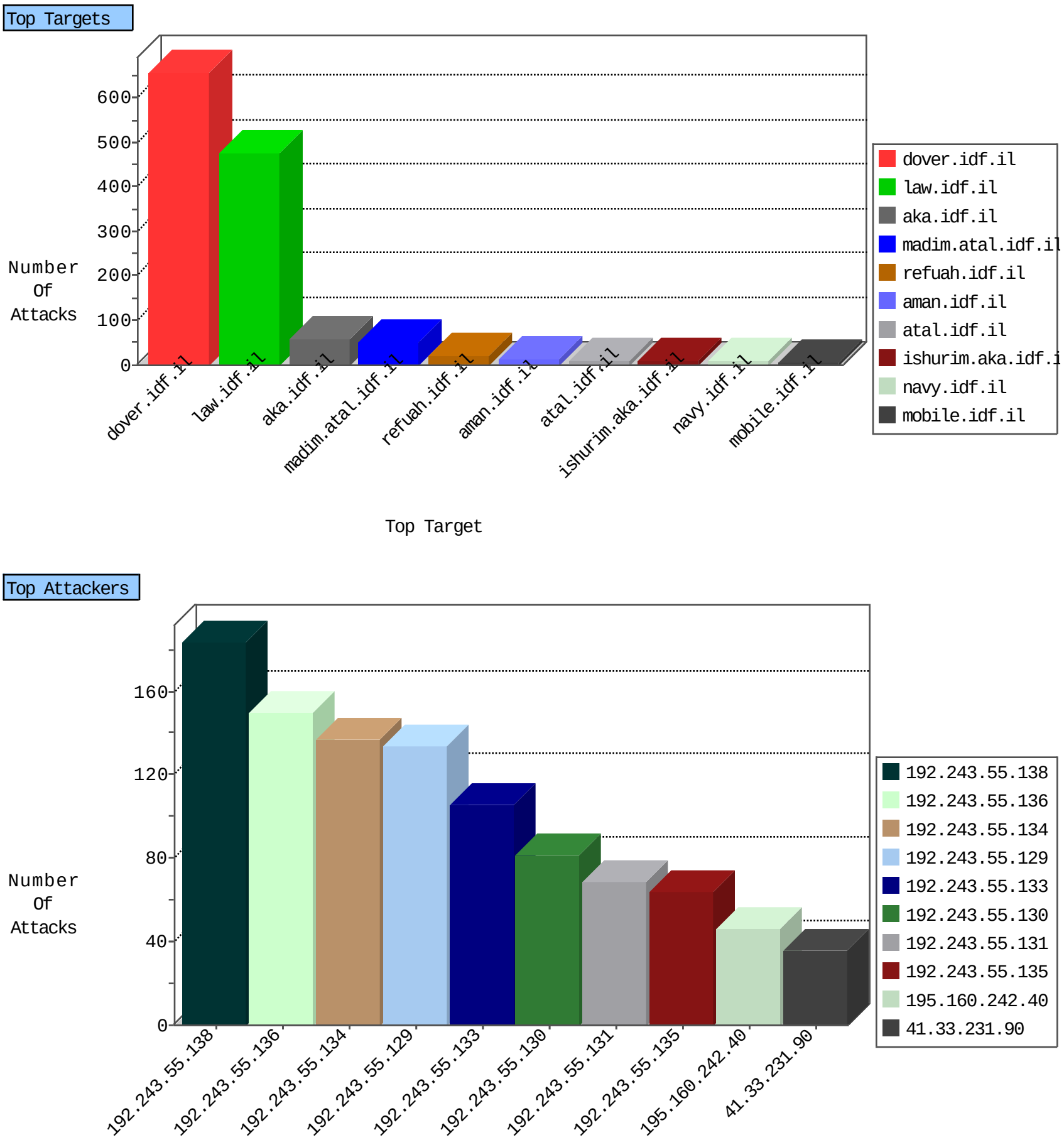
04-12-2016-07:04:00 to 04-12-2016-08:04:00

IDF Under Attack Daily Report



04-12-2016-07:04:00 to 04-12-2016-08:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.243.55.136	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	308
2.55.134.150	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	38
192.243.55.138	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	22
195.160.242.40	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
2.55.7.91	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
123.59.59.52	China	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
67.84.22.126	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
79.177.137.251	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
192.243.55.129	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
80.179.12.175	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
192.243.55.133	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
24.130.45.54	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
98.202.163.11	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-12-2016-07:04:00 to 04-12-2016-08:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
84.111.165.184	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-12-2016-07:04:00 to 04-12-2016-08:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.157.57.110	147.237.72.167	Sweden	ishurim.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
208.100.26.228	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
185.130.5.86	147.237.76.202	Lithuania	e.halag.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.86	147.237.76.42	Lithuania	refuah.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.86	147.237.72.14	Lithuania	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
108.233.78.156	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
41.214.25.190	147.237.0.200	Senegal	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
23.106.244.91	147.237.72.167	United States	ishurim.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
208.100.26.228	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.86	147.237.77.178	Lithuania	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.86	147.237.76.86	Lithuania	navy.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.86	147.237.76.31	Lithuania	nakchal.idf.il	ET SCAN Potential SSH Scan	1
185.125.216.75	147.237.77.170	Russian Federation	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.191	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.214.25.190	147.237.0.200	Senegal	m4u.idf.il	ET SCAN NMAP -sS window 1024	1

04-12-2016-07:04:00 to 04-12-2016-08:04:00

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
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
192.243.55.138	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
192.243.55.138	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	23
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
37.26.149.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	19
192.243.55.138	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
2.55.134.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
192.243.55.138	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
192.243.55.134	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	18
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
192.243.55.129	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
192.243.55.136	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
192.243.55.136	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
192.243.55.134	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
192.243.55.136	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
192.243.55.133	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
192.243.55.136	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
192.243.55.136	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	13
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
192.243.55.138	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
192.243.55.129	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.131	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.135	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.138	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
192.243.55.133	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
192.243.55.129	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
192.243.55.134	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.135	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.138	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.129	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
192.243.55.129	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.134	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
192.243.55.130	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	10
192.243.55.129	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.136	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
176.13.0.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 195.160.242.40	Block	7
46.19.86.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	5
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	3
46.19.86.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.30.16.172	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
112.213.117.30	Hong Kong	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
199.30.24.169	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.2.166	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.25.69	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.115.113.89	Block	2
199.30.25.108	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.16.166	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.45	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
23.106.244.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
112.213.117.30	Hong Kong	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 112.213.117.30	Block	1
80.246.133.110	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	1
207.46.13.62	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.65.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19559-he/dover.aspx	Block	1
192.243.55.138	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1225-	Block	1
130.185.155.82	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
104.251.82.167	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/shared/usercontrols/headerupper/	Block	1
2.55.150.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
79.180.60.2	Israel	147.237.76.39	mobile.meitav.idf.il	Cookie Tampering on cookie .ASPNETAUTH: Expected 0102B46D54B08762D308FEB4E5957B8A62D3080009330031003800350037003300310039003900330000012F00FF, Observed 01029A4CDA232E62D308FE9AC41BEF3062D3080009330031003800350037003300310039003900330000012F00FF	None	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/resources/styles/global.css	Block	1
23.106.244.91	United States	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
89.139.160.148	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/tmuna/	Block	1
131.253.25.222	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
54.92.161.185	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
5.157.57.110	Sweden	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
104.251.91.180	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/shared/usercontrols/lobbyinfocenteritem/	Block	1
80.227.144.220	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.223	Block	1
184.100.101.6	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/contribute.json	Block	1
37.187.114.171	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to /irj/portal	Block	1
112.213.117.30	Hong Kong	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
91.223.89.52	Ukraine	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/hnap1/	Block	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/eitan/listpage/	Block	1
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/sip_storage/files/7	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
62.4.22.224	France	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
23.80.148.35	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/228-he/faq.aspx	Block	1
109.67.184.116	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
80.227.144.220	United Arab Emirates	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.134	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/halochamim	Block	1
123.59.59.52	China	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.ctrip.com/894-he/chinuch.aspx	Block	1