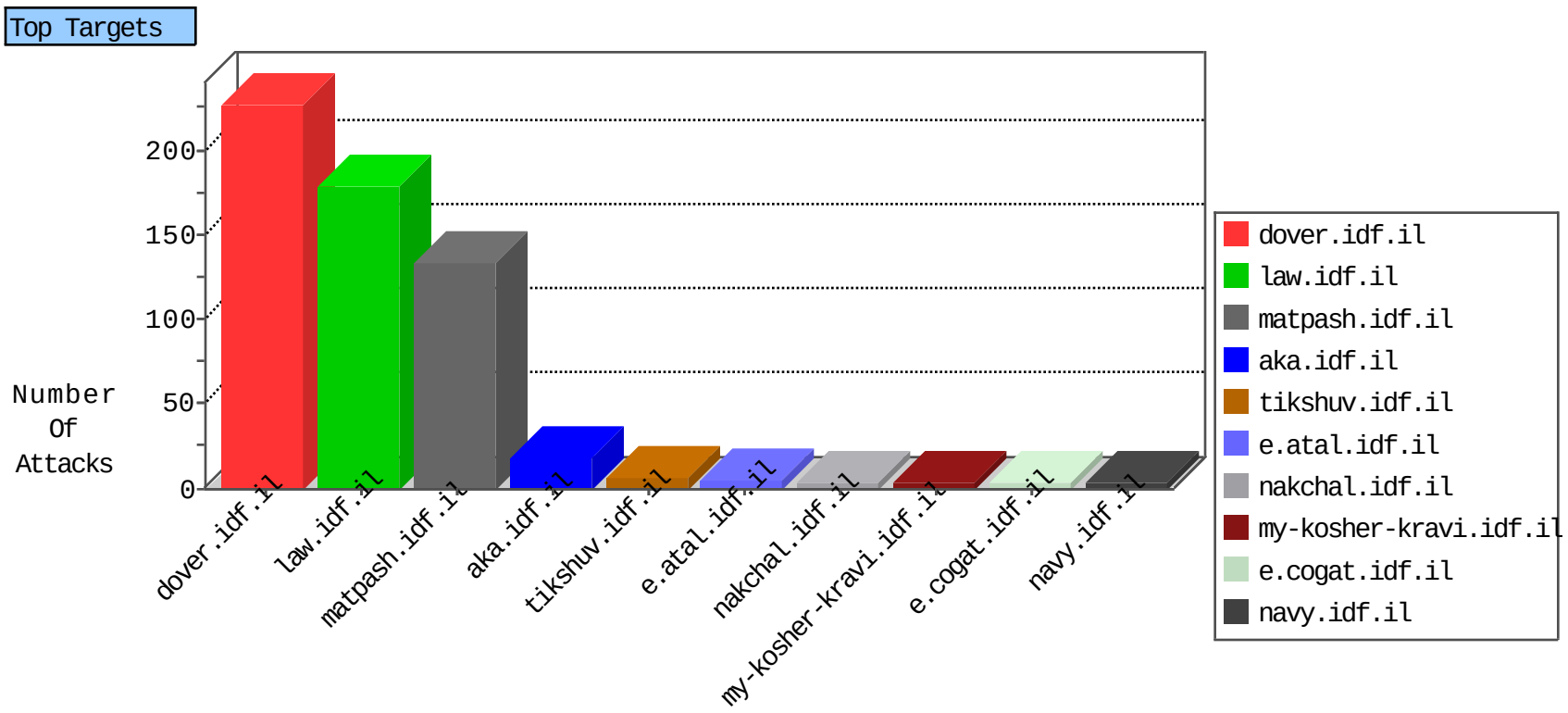
03-10-2016-05:04:09 to 03-10-2016-06:04:09

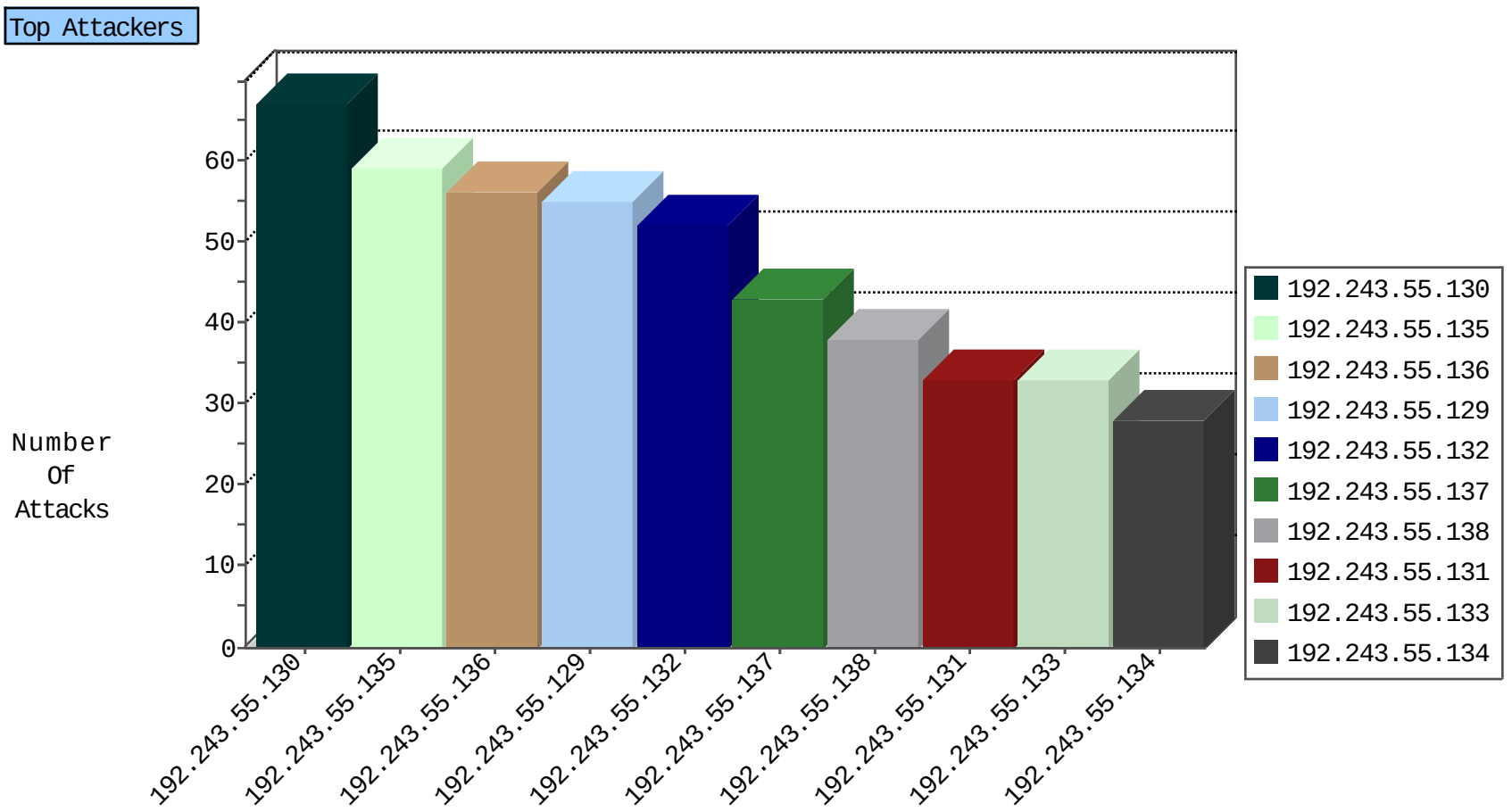
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

03-10-2016-05:04:09 to 03-10-2016-06:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
184.105.139.84	United States	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
85.25.43.218	Germany	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.77.212	e.dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.92	United States	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.207	Netherlands	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
71.6.135.131	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.116	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.84	United States	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
85.25.43.218	Germany	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
188.138.1.218	Germany	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.104	United States	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
162.212.72.1	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
85.25.43.218	Germany	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.124	United States	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
184.105.139.88	United States	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
85.25.43.218	Germany	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.104	United States	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.76	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
85.25.43.218	Germany	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.92	United States	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
85.25.43.218	Germany	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.104	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1

03-10-2016-05:04:09 to 03-10-2016-06:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.0.21	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	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	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-10-2016-05:04:09 to 03-10-2016-06:04:09

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
104.43.201.119	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
104.43.201.119	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
93.189.26.18	147.237.8.14	Austria	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
89.255.21.58	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
178.62.94.12	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
104.44.133.108	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 4096	1
104.43.201.119	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
104.43.201.119	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
104.43.201.119	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.142.166.43	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
218.246.0.97	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.245	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
178.62.94.12	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
178.62.94.12	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
104.44.133.108	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1

03-10-2016-05:04:09 to 03-10-2016-06:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
107.167.98.218	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.130	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.136	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.130	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.131	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.130	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.131	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.136	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.129	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.135	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.138	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	4
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.131	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.138	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.133	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.129	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

03-10-2016-05:04:09 to 03-10-2016-06:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.25.80	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
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.173	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.219	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.25.4	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
156.199.217.197		147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
65.55.210.228	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.232.29.186	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
185.12.108.247	Turkey	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 185.12.108.247	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
199.30.25.46	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
156.199.217.197		147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.232.29.186	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
185.12.108.247	Turkey	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.i	Unauthorized URL Access to www.tikshuv.idf.il/templates/contactus/contactus.aspx	Block	1
65.55.210.123	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
210.213.67.124	Philippines	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	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
207.232.29.186	Israel	147.237.76.31	nakchal.idf.i	Distributed PHP Attempt	Block	1
157.55.12.81	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
141.8.142.31	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	1
65.55.210.205	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.232.29.186	Israel	147.237.76.31	nakchal.idf.i	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	1
178.255.215.87	France	147.237.72.166	aka.idf.il	Unknown Parameter 287d8a30 in aka.idf.il/	None	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/5/71095.pdf	Block	1

03-10-2016-05:04:09 to 03-10-2016-06:04:09