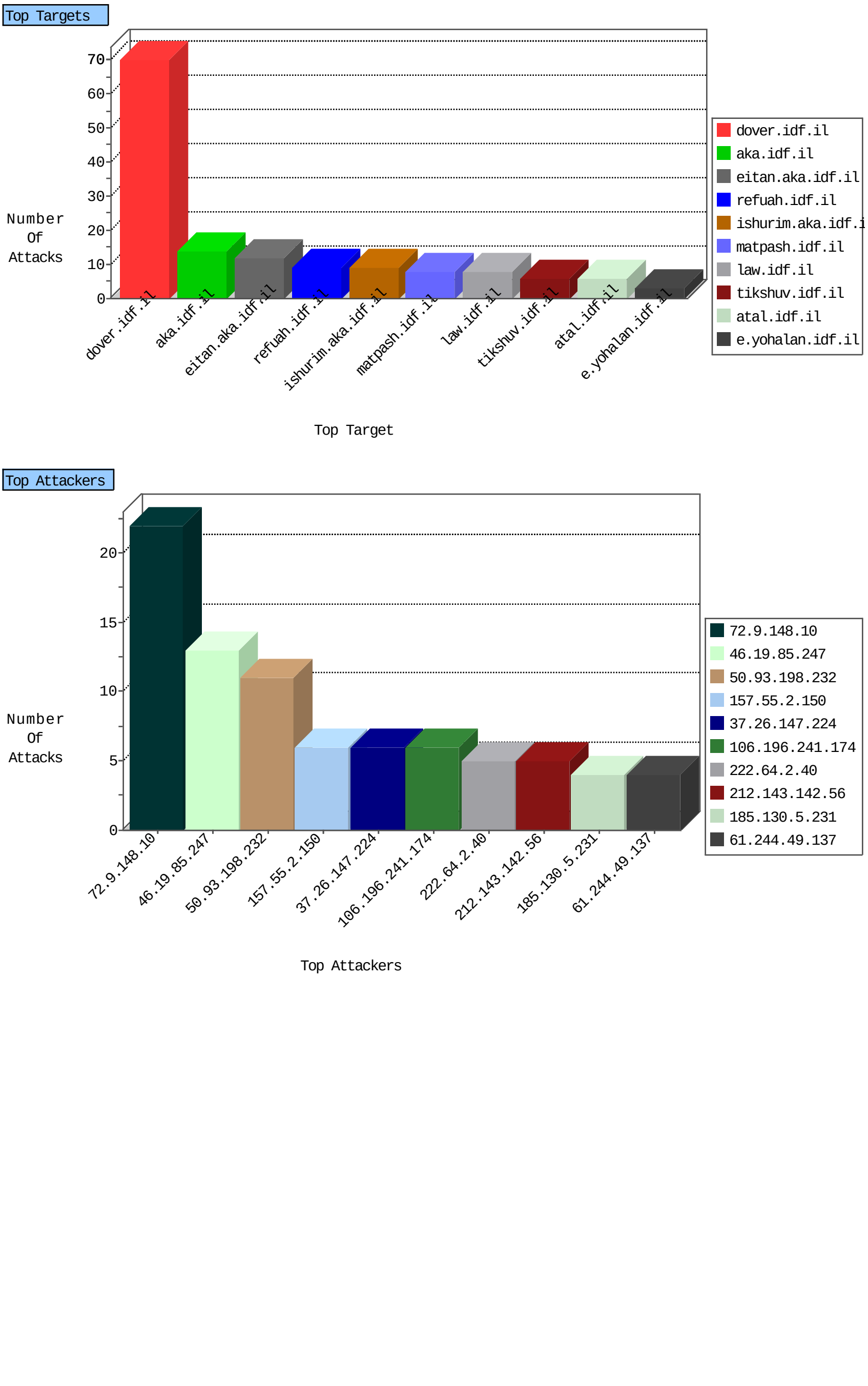
03-08-2016-05:04:08 to 03-08-2016-06:04:08

IDF Under Attack
Daily Report



03-08-2016-05:04:08 to 03-08-2016-06:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
71.6.216.37	United States	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.112	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.92	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.8.45	e.eitan.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.104	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.116	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.96	United States	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.108	United States	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.76	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.116	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.96	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
188.138.17.205	France	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.108	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.80	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
185.35.62.143	Switzerland	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.104	United States	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1

03-08-2016-05:04:08 to 03-08-2016-06:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.9.87.111	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.111	Italy	147.237.76.31	nakchal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
37.187.94.101	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.149	Italy	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
37.187.94.214	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
176.9.131.69	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	1
37.187.94.241	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
51.255.65.47	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-08-2016-05:04:08 to 03-08-2016-06:04:08

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
66.249.64.50	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
61.244.49.137	147.237.0.33	Hong Kong	idf.il	ET SCAN Potential SSH Scan	1
208.67.1.57	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.244.49.137	147.237.0.16	Hong Kong	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.77.61	Cote D'Ivoire	e.cogat.idf.il	ET SCAN NMAP -sS window 4096	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.231	147.237.77.170		maarachot.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.231	147.237.76.147		chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
72.252.24.133	147.237.8.45	Jamaica	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
61.244.49.137	147.237.0.34	Hong Kong	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
61.244.49.137	147.237.0.19	Hong Kong	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
201.172.102.164	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.77.61	Cote D'Ivoire	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
37.1.209.203	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.231	147.237.77.235		sviva.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.231	147.237.76.200		eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
117.5.89.36	147.237.77.205	Vietnam	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
85.93.5.66	147.237.76.31	Germany	nakchal.idf.il	ET SCAN Potential SSH Scan	1

03-08-2016-05:04:08 to 03-08-2016-06:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
46.19.85.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
157.55.2.150	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
106.196.241.174	India	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
37.26.147.224	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
109.253.209.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.218.11.69	Switzerland	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
199.30.25.98	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
222.64.2.40	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
24.13.150.70	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
146.185.239.102	Russian Federation	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
50.93.198.232	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
216.218.206.92	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
186.188.105.202	Venezuela	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.150	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
222.64.2.40	China	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
50.93.198.232	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
37.26.147.158	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
50.93.198.232	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
216.218.206.120	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
50.93.198.232	United States	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
190.232.113.6	Peru	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.151	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
50.93.198.232	United States	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
212.96.50.6	Hungary	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
180.76.15.27	China	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
50.93.198.232	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
218.22.211.69	China	147.237.0.35	akaws.idf.il	drop		drop	1
50.93.198.232	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
190.232.113.6	Peru	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.158	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
50.93.198.232	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
212.96.50.6	Hungary	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.46.41.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.114	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
130.193.51.73	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
51.254.44.137	United Kingdom	147.237.0.33	idf.il	drop		drop	1
222.64.2.40	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
50.93.198.232	United States	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
190.232.113.6	Peru	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.159	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
50.93.198.232	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
184.105.247.239	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
137.116.71.170	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
51.254.44.137	United Kingdom	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

03-08-2016-05:04:08 to 03-08-2016-06:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
196.46.186.134	South Africa	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SortDir in www.eitan.aka.idf.il/1103-en/eitan.aspx	None	1
40.77.167.36	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
166.62.35.111	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
66.249.64.61	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
222.64.2.40	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
107.6.153.58	Netherlands	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 107.6.153.58	Block	1
40.77.167.75	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
183.111.174.4	Korea, Republic of	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
66.249.64.153	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/imagevideogallerylobby/imagevideogallerylobby.aspx	Block	1
107.6.153.58	Netherlands	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
185.45.13.162	Romania	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
122.2.110.50	Philippines	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
195.138.85.250	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/sendtofriend.aspx?&amp	Block	1
66.249.73.190	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
37.26.149.244	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
122.2.110.50	Philippines	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	1

03-08-2016-05:04:08 to 03-08-2016-06:04:08