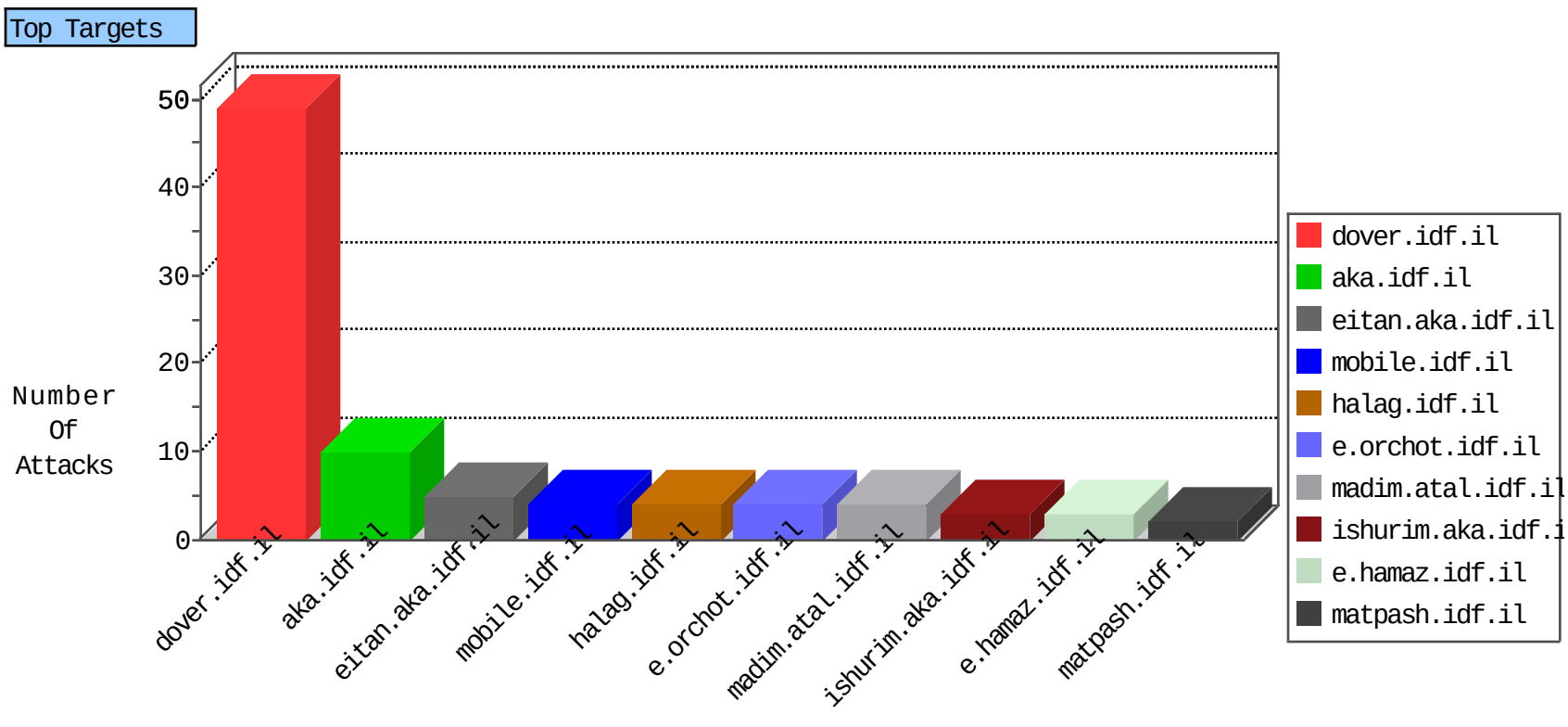
03-10-2016-04:04:06 to 03-10-2016-05:04:06

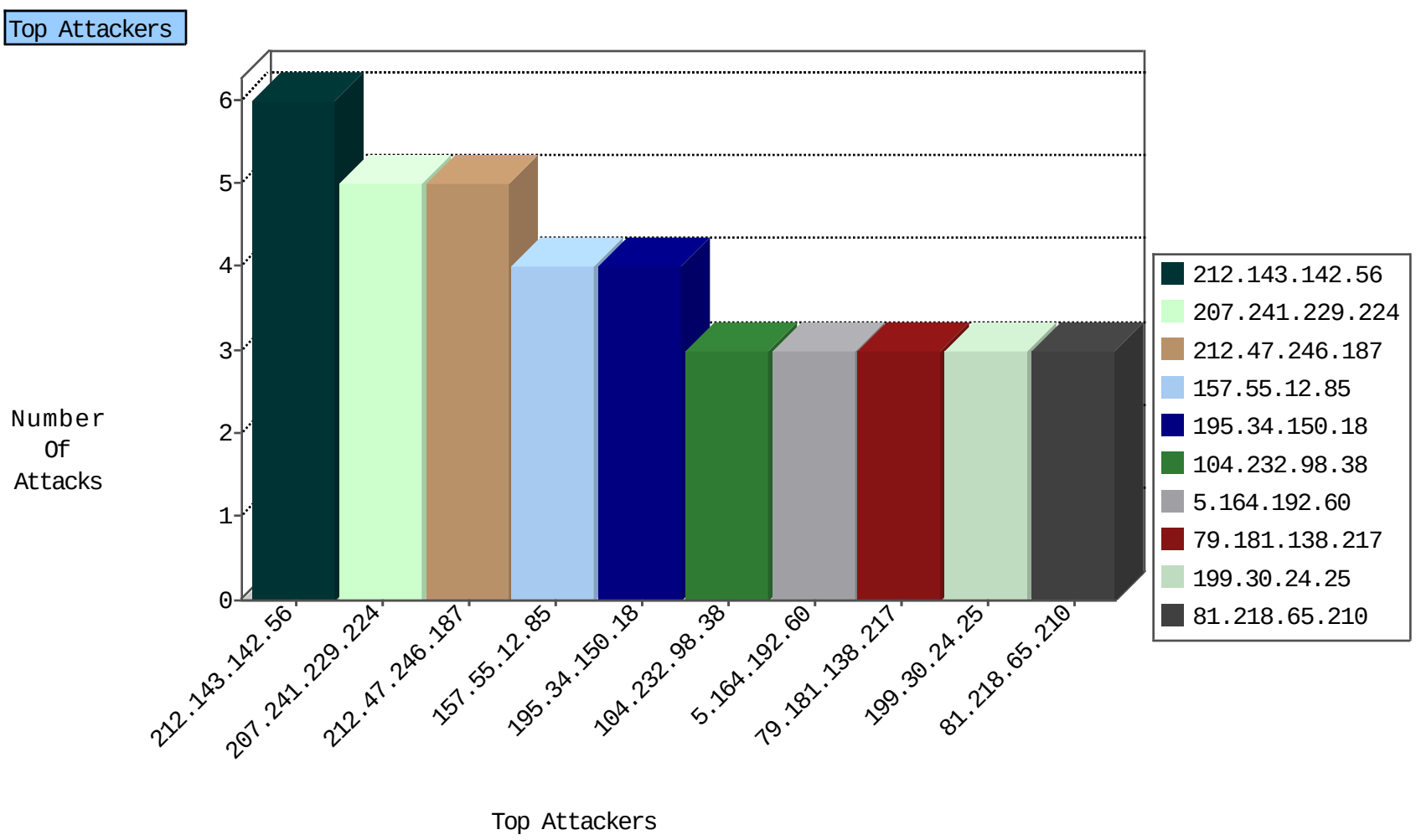
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

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

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
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
216.218.206.67	United States	147.237.77.178	e.matpash.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.207	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
216.218.206.111	United States	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	1
71.6.135.131	United States	147.237.77.243	mobile.idf.il	Block_Udp_All_Nets	drop	1
95.170.21.51	France	147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	1
216.218.206.111	United States	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1
71.93.222.191	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
162.216.114.158	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.211	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.66.187	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
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

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

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
104.232.98.38	147.237.8.14		e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
104.232.98.38	147.237.8.14		e.orchot.idf.il	ET SCAN NMAP -f -sS	1
104.44.133.108	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.38	147.237.8.14		e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
104.44.133.108	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
93.189.26.18	147.237.0.35	Austria	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
208.67.1.147	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.241.229.224	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.164.192.60	Russian Federation	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	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
212.47.246.187	France	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.94	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.146	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.34	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
176.126.252.12	Romania	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
109.163.234.2	Romania	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
46.19.86.244	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
212.47.246.187	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.102	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.146	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.35	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.47.246.187	France	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
178.162.205.1	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
123.126.113.80	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
62.216.235.12	United Kingdom	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.106	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.149	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.35	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.47.246.187	France	147.237.0.35	akaws.idf.il	drop		drop	1
184.105.139.80	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.145	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.112	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.235	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.150	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.178.114.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
212.47.246.187	France	147.237.76.34	yohalan.idf.il	drop		drop	1
184.105.139.94	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.145	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.16	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
221.199.217.173	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.240	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
171.25.193.25	Sweden	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
80.178.114.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

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

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
157.55.12.85	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
199.30.24.25	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.24.69	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
79.181.138.217	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
199.30.25.88	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.146	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.2.151	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.163.234.2	Romania	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
46.19.86.244	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	1
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
207.241.229.224	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/general/general.aspx	Block	1
131.253.25.140	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
172.56.31.143	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
213.49.118.85	Belgium	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
156.199.217.197		147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.220.156.117	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.12.48.184	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
213.49.118.85	Belgium	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
156.199.217.197		147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.164.192.60	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/	Block	1
66.249.65.232	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1

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