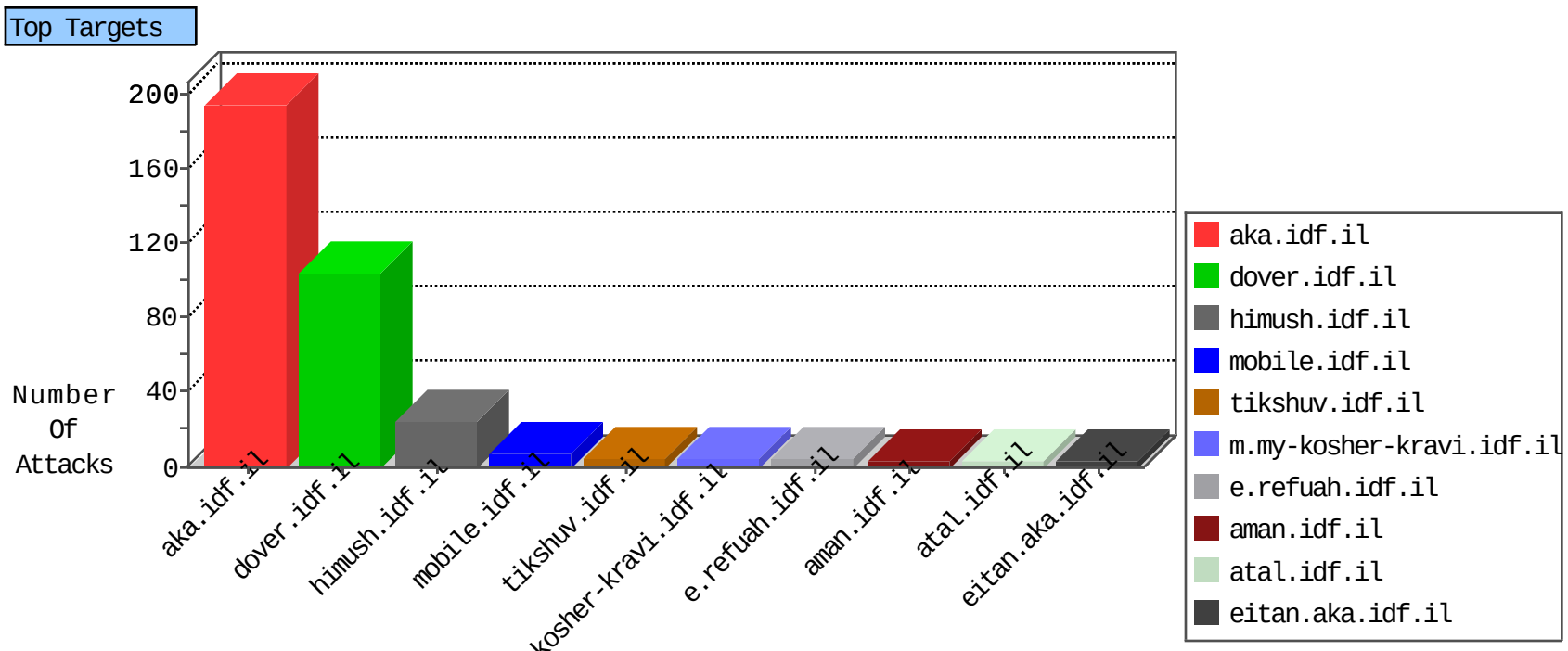
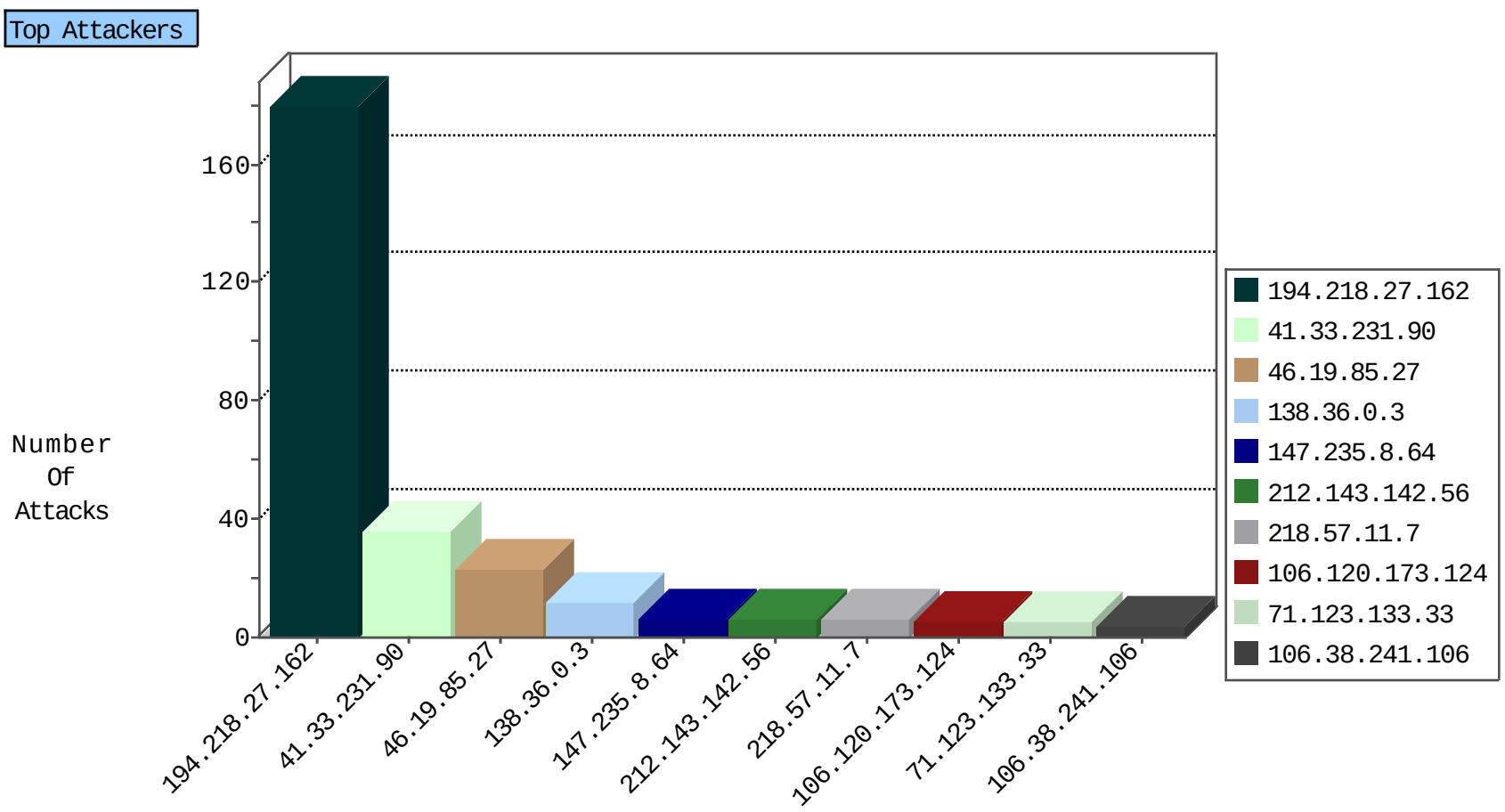
02-29-2016-03:04:01 to 02-29-2016-04:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-29-2016-03:04:01 to 02-29-2016-04:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
185.35.62.127	Switzerland	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
162.216.114.158	United States	147.237.8.24	e.lifestyle.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.129	Switzerland	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
175.124.212.146	Korea, Republic of	147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.201		147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
62.8.70.58	Kenya	147.237.77.121	e.navy.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.125	Switzerland	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
188.138.102.50	Germany	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1
62.8.70.58	Kenya	147.237.77.227	e.hamaz.idf.il	Block_Udp_All_Nets	drop	1

02-29-2016-03:04:01 to 02-29-2016-04:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.124	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
66.249.64.180	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
66.249.64.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

02-29-2016-03:04:01 to 02-29-2016-04:04:01

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
66.249.79.10	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
71.84.230.42	147.237.76.30	United States	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.57.11.7	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
59.148.90.11	147.237.8.28	Hong Kong	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.57.11.7	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.249	147.237.76.202		e.halag.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.118	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.8.46		e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
218.57.11.7	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.77.212	Sweden	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.249	147.237.76.200		eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.118	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.117.186.51	147.237.72.14	Spain	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

02-29-2016-03:04:01 to 02-29-2016-04:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	118
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	59
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.85.27	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
71.123.133.33	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
185.27.106.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.215.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.77	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
37.26.148.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.133	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
147.235.8.64	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
147.235.8.64	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
207.46.13.70	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
147.235.8.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
123.125.71.90	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
85.248.227.163	Slovakia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
159.226.95.66	China	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.78	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
138.36.0.3		147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
194.150.168.79	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
106.38.241.106	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
171.25.193.77	Sweden	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
138.36.0.3		147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.20.69.98	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
138.36.0.3		147.237.76.197	e.himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.100.85.190		147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
93.115.95.204	Anonymous Proxy	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
169.54.233.124	Netherlands	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	1
68.11.205.168	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.172	United States	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
138.36.0.3		147.237.77.212	e.dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.163.234.9	Romania	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
176.126.252.12	Romania	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
46.121.64.15	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
138.36.0.3		147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
138.36.0.3		147.237.76.198	e.yohalan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
193.90.12.86	Norway	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
95.130.12.37	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
169.54.233.124	Netherlands	147.237.72.14	dover.idf.il(old)	drop	First packet isn't SYN	drop	1
68.11.205.168	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.173	United States	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.187.119.59	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
138.36.0.3		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
114.112.90.54	China	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
178.32.53.53	United Kingdom	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
80.244.81.191	Sweden	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
62.210.105.116	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1

02-29-2016-03:04:01 to 02-29-2016-04:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.118.114.75	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	3
131.253.25.168	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	3
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	3
66.249.66.21	United States	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.66.21	Block	3
66.249.64.143	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
67.19.79.218	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /robots.txt	Block	1
66.249.64.229	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1232-he/atal.aspx	Block	1
193.90.12.88	Norway	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
66.249.66.21	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1674	Block	1
66.249.66.12	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/108889.pdf	Block	1
157.55.39.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.15	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1722	Block	1
66.249.69.32	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19163-he/dover.aspx	Block	1
66.249.64.149	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
184.105.247.196	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.66.18	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1734	Block	1
66.249.78.80	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
66.249.64.190	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/general.aspx	Block	1
185.112.248.32		147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1

02-29-2016-03:04:01 to 02-29-2016-04:04:01