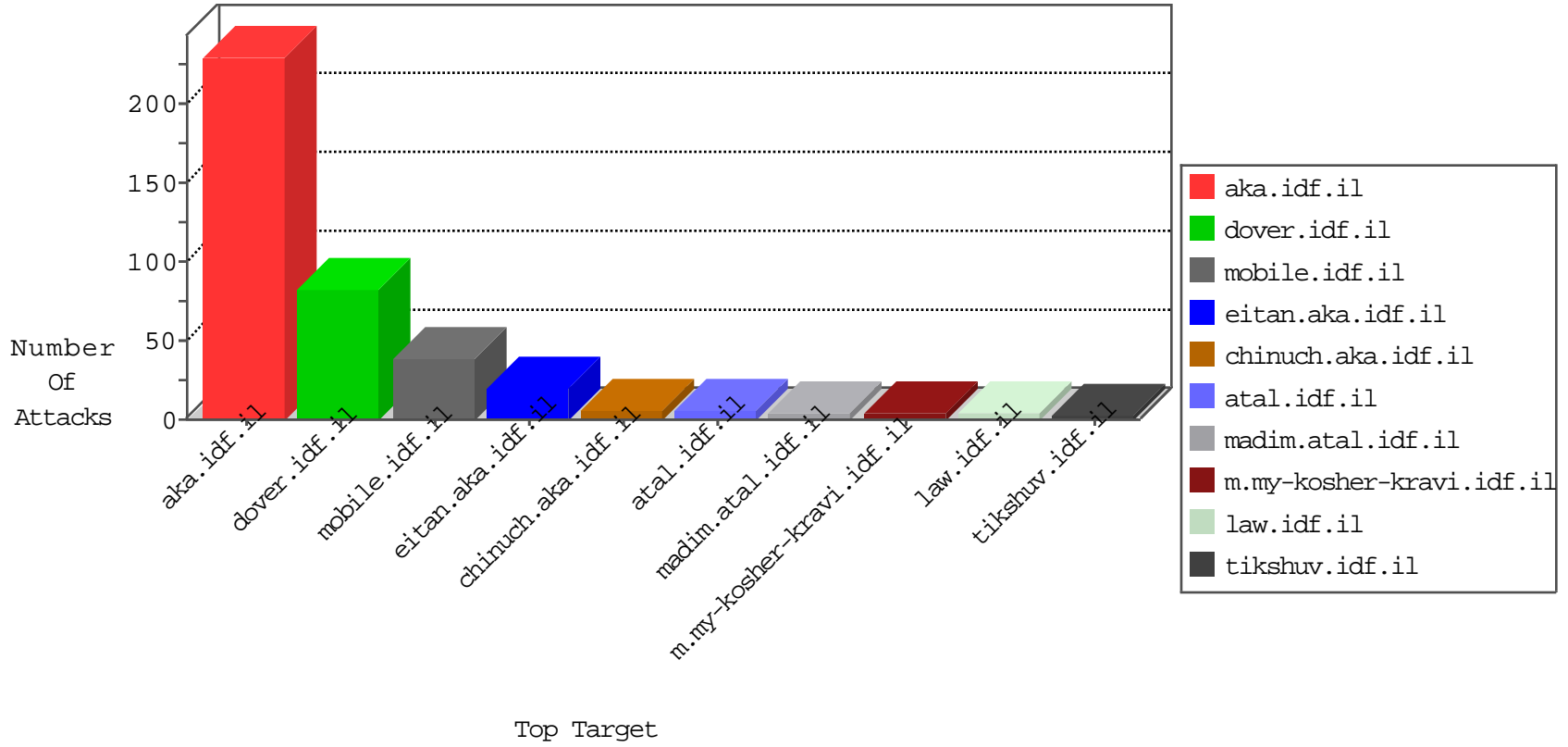


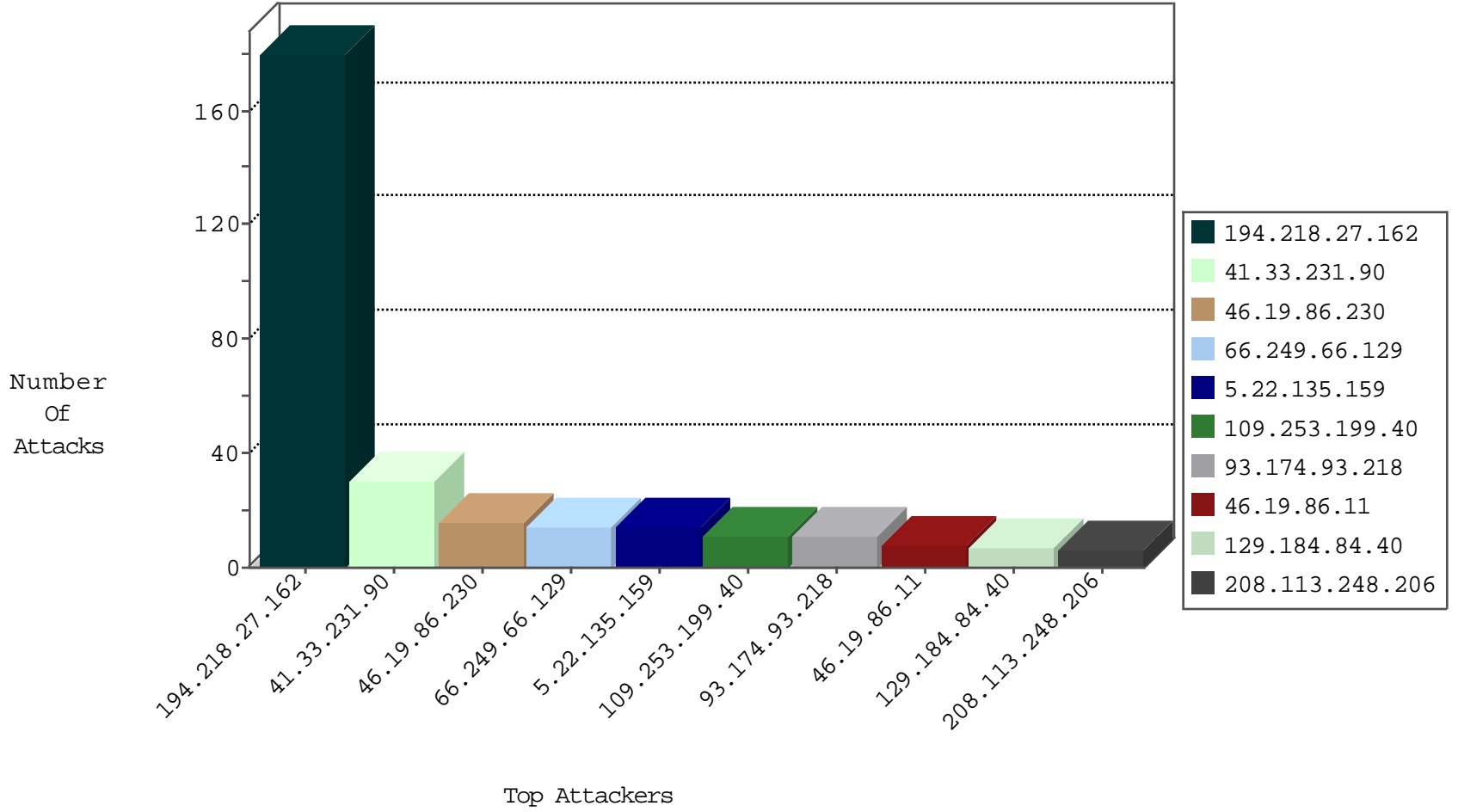
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	8
82.145.222.181	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
93.174.93.218	Netherlands	147.237.72.166	aka.idf.il	block-sp-traf1	drop	2
185.130.5.224		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
10.8.0.38		147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
185.130.5.224		147.237.77.212	e.dover.idf.il	Block_Udp_All_Nets	drop	1
23.239.64.15	United States	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.33	Switzerland	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
72.142.18.42	Canada	147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.201		147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	1

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
66.249.64.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

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
186.182.100.172	147.237.76.30	Argentina	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.130.5.249	147.237.72.217		e.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.249	147.237.0.34		tikshuv.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.249	147.237.0.15		kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.118	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
189.219.113.163	147.237.8.14	Mexico	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.130.5.249	147.237.76.34		yochalan.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.249	147.237.0.200		m4u.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.249	147.237.0.19		madim.atal.idf.il	ET SCAN Potential SSH Scan	1
164.39.11.198	147.237.0.200	United Kingdom	m4u.idf.il	ET SCAN NMAP -sS window 1024	1

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	30
66.249.66.129	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
46.19.86.230	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.199.40	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.11	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.79.10	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.135.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.135.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.253.144.172	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.99.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.0.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.27.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.158.152.49	Russian Federation	147.237.76.147	chimuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.102.8.137	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	3
5.22.135.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
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
66.249.66.137	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
93.174.93.218	Netherlands	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
154.20.47.147	Canada	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
141.212.122.69	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
207.46.13.139	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
157.55.39.4	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
195.62.53.168	Russian Federation	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.70	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
169.54.244.84	Netherlands	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	1
114.112.90.54	China	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
66.102.8.131	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	1
195.62.53.168	Russian Federation	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.78	United States	147.237.76.147	chimuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.38.241.106	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
169.54.244.84	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.64	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
195.62.53.168	Russian Federation	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.79	United States	147.237.76.147	chimuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.38.241.106	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
78.46.97.213	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.65	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
198.20.69.74	United States	147.237.8.27	e.madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
129.184.84.40	France	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	6
208.113.248.206	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 208.113.248.206	Block	5
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	5
46.19.86.230	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
93.174.93.218	Netherlands	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 93.174.93.218	Block	3
109.253.199.40	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
93.174.93.218	Netherlands	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 93.174.93.218	Block	2
46.19.86.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.80	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
157.55.39.183	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
66.249.64.137	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
66.249.78.94	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
46.121.232.235	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cpMain\$TochenPlaceHolder\$btnAtudaBack in www.aka.idf.il/main/gyus/atuda/asmachta.aspx	None	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20232-he/kkkkkkk=79615652kkkkkkk_79615652	Block	1
66.249.66.21	United States	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.66.21	Block	1
129.184.84.40	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	1
52.48.17.30	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
93.174.93.218	Netherlands	147.237.72.166	aka.idf.il	NULL Character in Method	Block	1
66.249.66.21	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1735	Block	1
46.19.86.11	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
141.212.122.64	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to /x	Block	1
81.223.254.34	Austria	147.237.77.234	halag.idf.il	Unauthorized URL Access to /robots.txt	Block	1
54.196.162.63	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/brothers/skira/default.asp	Block	1
208.113.248.206	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
109.227.90.27	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	1
141.212.122.64	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to /x	Block	1
93.174.93.218	Netherlands	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method	Block	1
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1