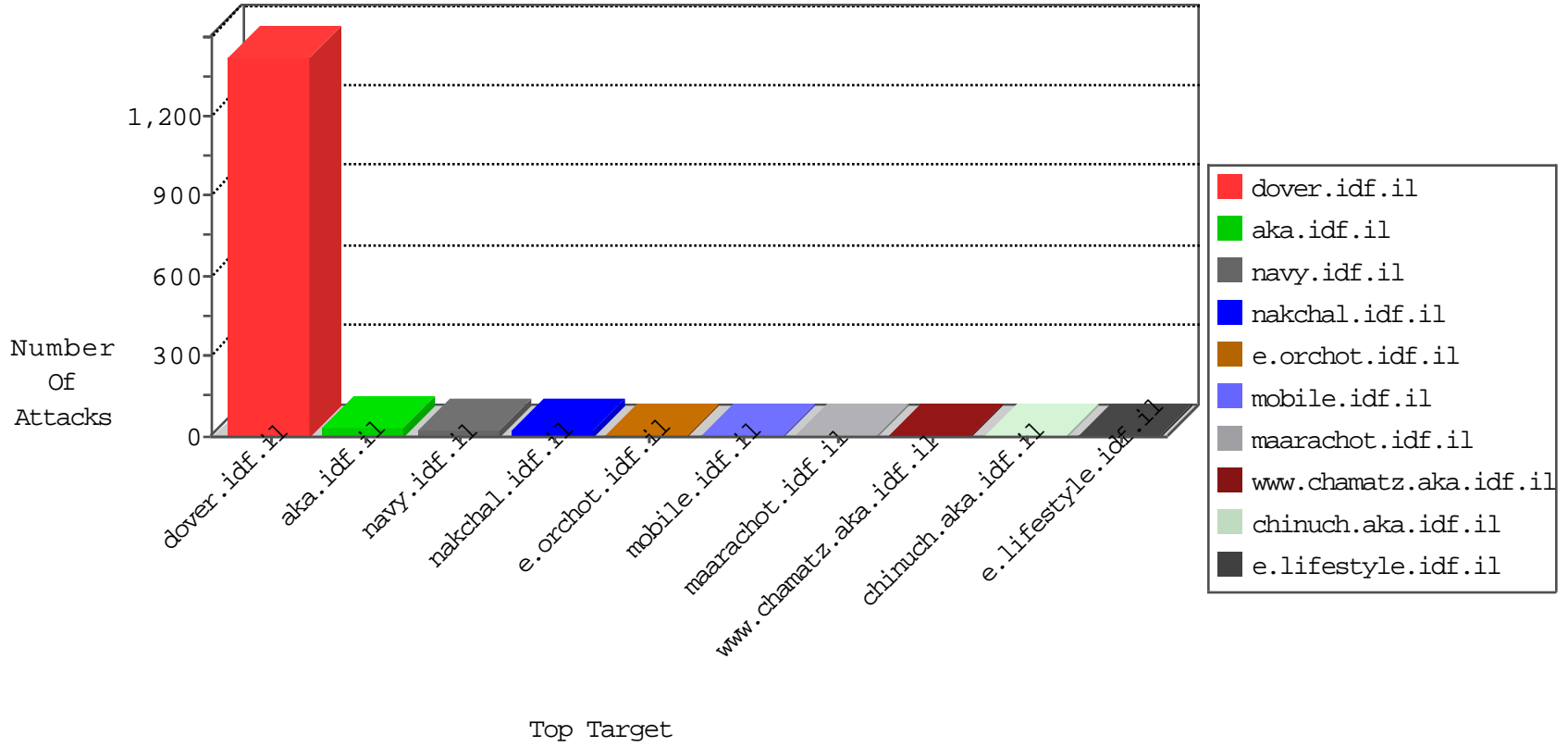


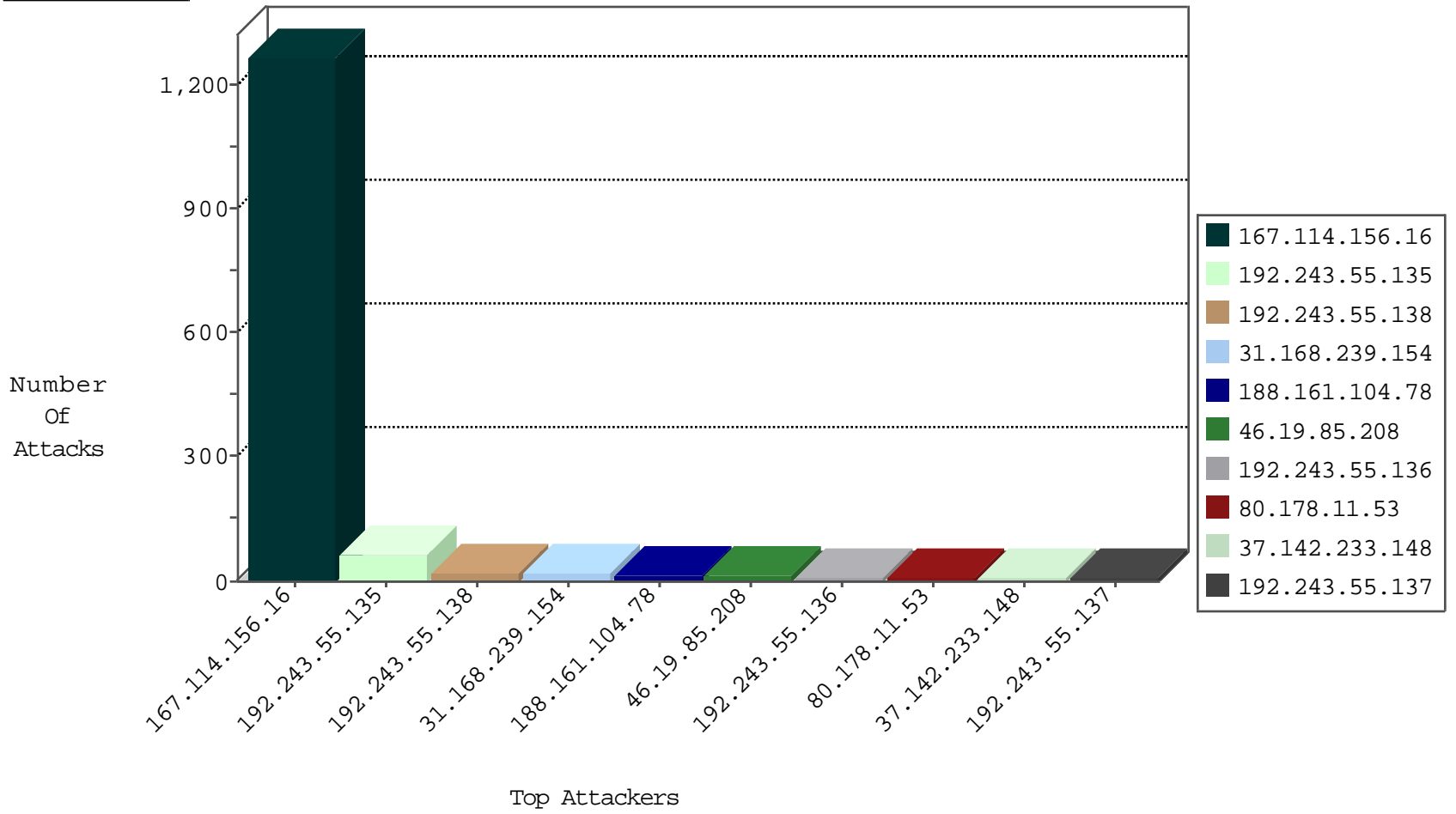
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3979
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
126.46.7.121	Japan	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.94	United States	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
162.248.100.195	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
58.97.74.88	Thailand	147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	1
209.126.102.181	United States	147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.33	Switzerland	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
162.248.100.195	United States	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.110	United States	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
162.248.100.195	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
216.218.206.75	United States	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.67	United States	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1
162.248.100.195	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.118	United States	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.206	Netherlands	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.78	United States	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
162.248.100.195	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.122	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.33	Switzerland	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.65.248	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
104.45.226.46	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
164.39.11.198	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
104.197.254.53	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1
104.197.254.53	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -f -sS	1
104.45.226.46	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
104.45.226.46	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.34	China	yochalan.idf.il	ET SCAN NMAP -sS window 1024	1
185.110.132.54	147.237.76.197		e.himush.idf.il	ET SCAN Potential SSH Scan	1
164.39.11.198	147.237.8.14	United Kingdom	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
104.197.254.53	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
104.45.226.46	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	23
31.168.239.154	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.85.208	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
188.161.104.78	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
80.178.11.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.65.123.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.20.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.18.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.68.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.142.233.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.179.166.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.142.233.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
188.120.154.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
188.161.104.78	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
31.168.239.154	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	2
188.161.104.78	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
84.108.136.72	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
188.120.154.107	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
52.53.235.116	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
85.65.29.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
54.193.81.204	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
87.70.44.112	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
188.161.104.78	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.119.167.19		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
220.181.108.147	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.120.44.35	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
85.64.179.226	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.60	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.76.15.24	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
158.58.188.211	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.85.66	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
89.139.128.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
54.244.22.103	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.34	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1273-he/atal.aspx	Block	1
89.190.50.92	Czech Republic	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/2973.jpg	Block	1
207.46.13.100	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
66.249.66.125	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/shared/usercontrols/headerupper/	Block	1
141.212.122.160	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
66.249.64.124	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
80.178.11.53	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
37.46.41.237	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
178.20.55.16	France	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
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
89.138.124.207	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct151 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
37.237.240.85	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1