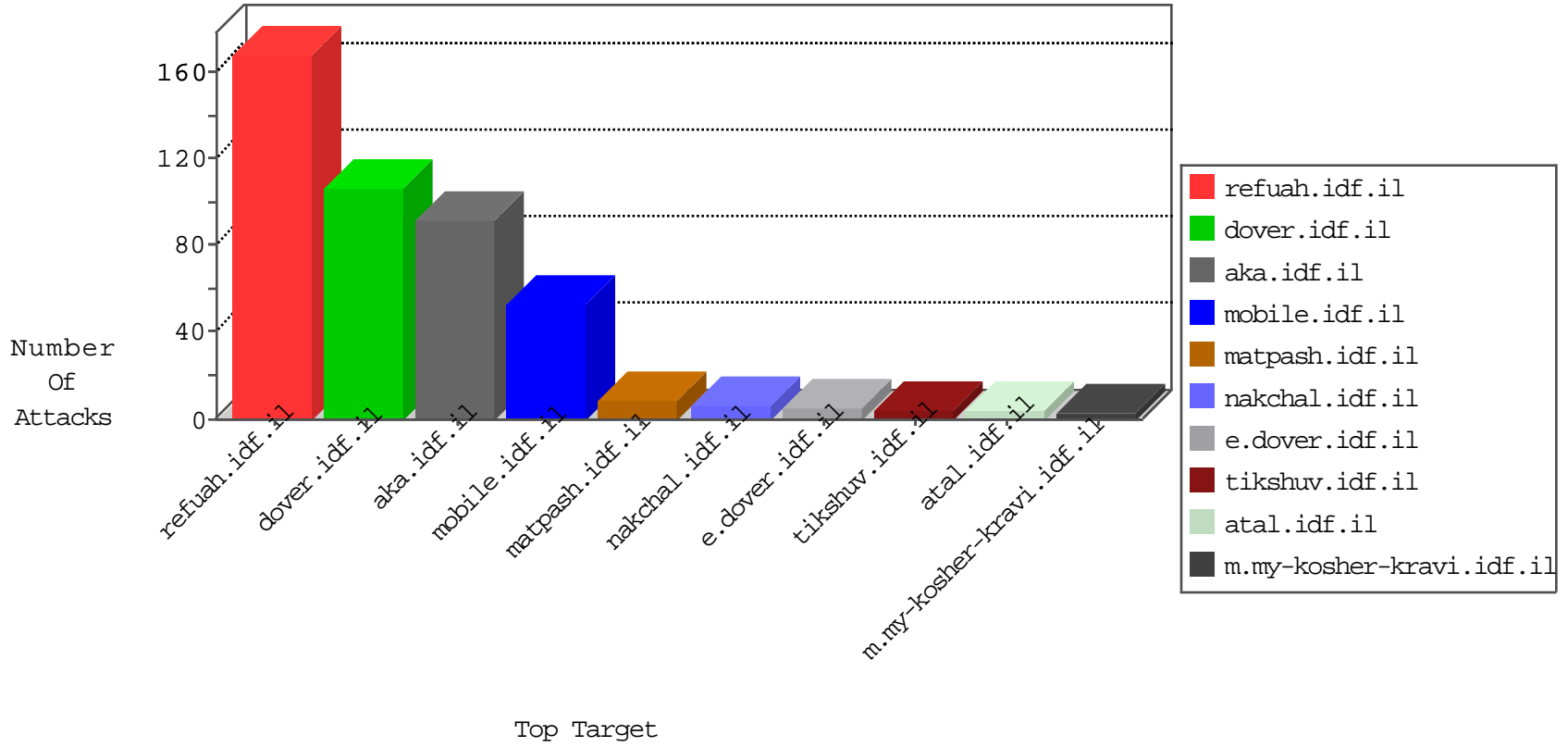


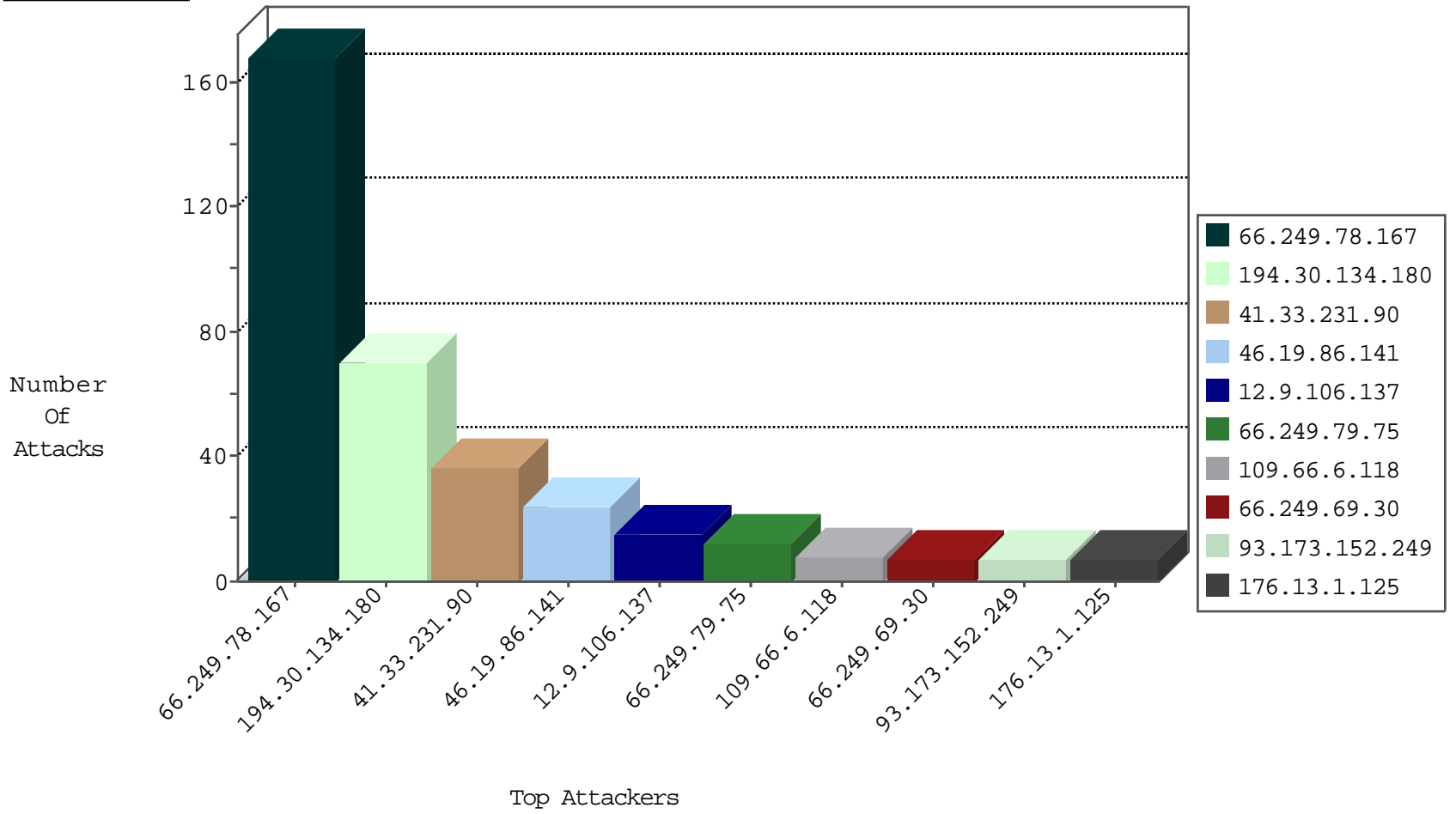
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	2
105.155.42.114	Morocco	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
179.43.144.33	Switzerland	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
115.239.228.10	China	147.237.0.34	tikshuv.idf.il	JLM_Purple_Con_Limit_Http	drop	1
185.130.5.231		147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1
205.209.185.11	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.33	Switzerland	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
162.210.196.97	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
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	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.167	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	168
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.66.39	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
12.9.106.137	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
12.9.106.137	147.237.72.166	United States	aka.idf.il	ET SCAN Potential SSH Scan	1
12.9.106.137	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
179.182.58.195	147.237.77.212	Brazil	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
12.9.106.137	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
12.9.106.137	147.237.77.233	United States	atal.idf.il	ET SCAN Potential SSH Scan	1
12.9.106.137	147.237.77.212	United States	e.dover.idf.il	ET SCAN Potential SSH Scan	1
12.9.106.137	147.237.77.19	United States	law-forum.idf.il	ET SCAN Potential SSH Scan	1
12.9.106.137	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
12.9.106.137	147.237.76.148	United States	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
12.9.106.137	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
12.9.106.137	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
179.182.58.195	147.237.77.212	Brazil	e.dover.idf.il	ET SCAN NMAP -f -sS	1
12.9.106.137	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
12.9.106.137	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
12.9.106.137	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
12.9.106.137	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
194.30.134.180	Cyprus	147.237.72.166	aka.idf.il	drop	SAM rule	drop	70
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.86.141	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.66.6.118	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
66.249.69.30	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.173.152.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.1.125	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.73.250	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.46.39.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.154.173.103	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
71.224.195.47	United States	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
109.253.143.232	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.24	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
197.160.83.53	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
84.94.63.157	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
24.237.158.6	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
182.118.21.219	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.155.131.76	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
74.82.47.55	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.154.173.103	France	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
184.105.139.103	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.243	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
197.160.83.53	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
184.105.247.239	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.74	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.80	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
80.244.81.191	Sweden	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.139.108	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
146.185.239.102	Russian Federation	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
93.115.95.205	Anonymous Proxy	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
199.27.242.227	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
188.138.9.49	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
38.229.1.15	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.83	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.82	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.126	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
162.247.72.217	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
199.27.242.227	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.34	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
38.229.1.15	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.99	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
216.218.206.90	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.94.63.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
197.160.83.53	Egypt	147.237.77.216	dover.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
66.249.79.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.75	Block	12
207.46.13.133	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluum/common/includes/bignewsrnd.asp	Block	1
69.244.85.145	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/en-espanolaspx	Block	1
46.19.86.24	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
120.28.191.4	Philippines	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.178.16.101	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.119	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
120.28.191.5	Philippines	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.83.158	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.178.35.113	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
66.249.64.234	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
120.28.191.6	Philippines	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
80.244.81.191	Sweden	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
66.249.66.69	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/moreinfo/tichnun.yosh@gmail.com	Block	1
176.13.1.125	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
38.229.1.15	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
93.173.152.249	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.30	United States	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	1