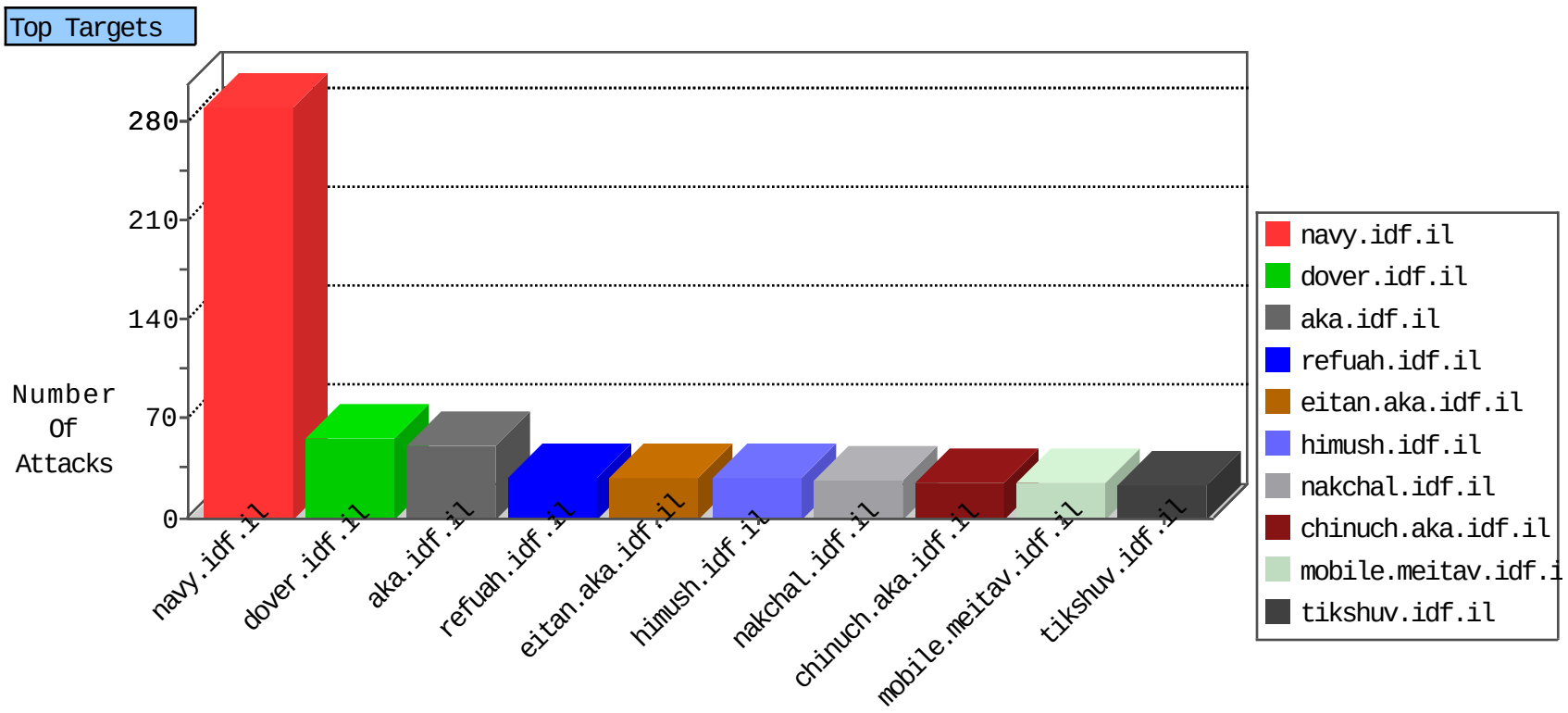
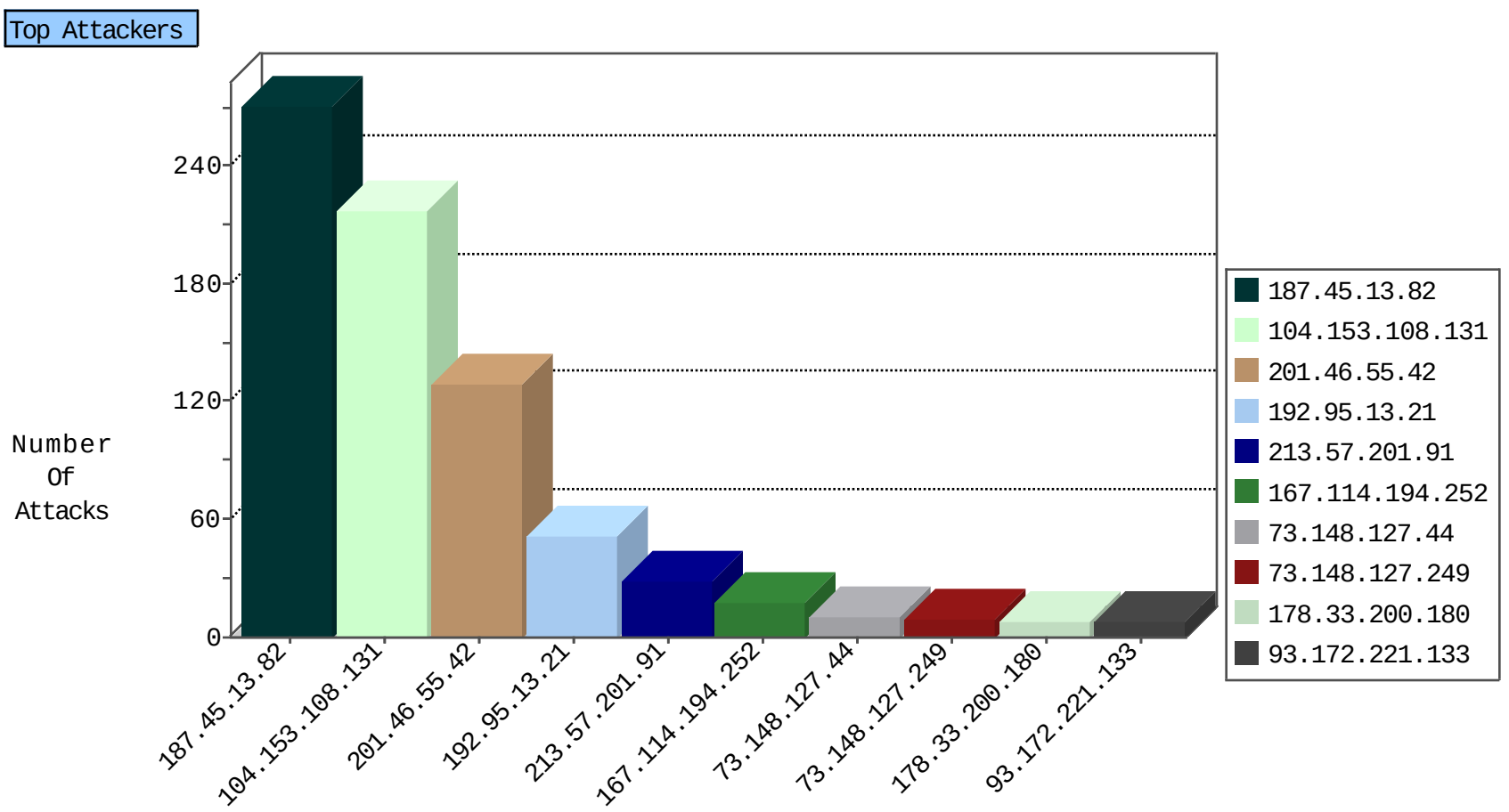
09-10-2016-04:04:06 to 09-10-2016-05:04:06

IDF Under Attack Daily Report





09-10-2016-04:04:06 to 09-10-2016-05:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Black List	drop	1
94.177.164.99	Romania	147.237.76.86	navy.idf.il	Black List	drop	1
179.104.41.73	Brazil	147.237.72.14	dover.idf.il(old)	JLM_Purple_Con_Limit_Tcp	drop	1
185.81.158.121	France	147.237.76.44	e.refuah.idf.il	Black List	drop	1

09-10-2016-04:04:06 to 09-10-2016-05:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
178.33.200.180	France	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Permit	8

09-10-2016-04:04:06 to 09-10-2016-05:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
71.6.216.41	147.237.77.170	United States	maarachot.idf.il	ET SCAN Potential SSH Scan	1
69.24.208.162	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.77.19	United States	law-forum.idf.il	ET DROP Dshield Block Listed Source	1
24.173.213.138	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
191.101.251.160	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
167.0.255.151	147.237.77.121	Colombia	e.navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.129.15	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.23.201.8	147.237.0.35	Malaysia	akaws.idf.il	ET SCAN NMAP -sS window 4096	1
103.207.37.82	147.237.77.212	Vietnam	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
69.24.208.162	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
40.85.252.239	147.237.0.19	Canada	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
195.88.208.193	147.237.72.167	Russian Federation	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
176.47.46.123	147.237.77.176	Saudi Arabia	matpash.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
163.172.129.15	147.237.76.31	United Kingdom	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
139.162.168.200	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
113.23.201.8	147.237.0.35	Malaysia	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

09-10-2016-04:04:06 to 09-10-2016-05:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
104.153.108.131	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	97
104.153.108.131	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	36
104.153.108.131	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
104.153.108.131	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	30
213.57.201.91	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	29
104.153.108.131	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	24
187.45.13.82	Brazil	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
187.45.13.82	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
187.45.13.82	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
187.45.13.82	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
187.45.13.82	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
187.45.13.82	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
187.45.13.82	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
187.45.13.82	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
187.45.13.82	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
187.45.13.82	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
187.45.13.82	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
187.45.13.82	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
187.45.13.82	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
187.45.13.82	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
187.45.13.82	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
187.45.13.82	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
187.45.13.82	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
201.46.55.42	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
201.46.55.42	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
187.45.13.82	Brazil	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
187.45.13.82	Brazil	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
201.46.55.42	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
201.46.55.42	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
201.46.55.42	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
201.46.55.42	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
187.45.13.82	Brazil	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
201.46.55.42	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
201.46.55.42	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
187.45.13.82	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
187.45.13.82	Brazil	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
93.172.221.133	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
95.146.187.116	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
141.0.13.234	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
201.46.55.42	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
201.46.55.42	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
73.148.127.249	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
201.46.55.42	Brazil	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
201.46.55.42	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
73.148.127.44	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
201.46.55.42	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
201.46.55.42	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
73.148.127.249	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
201.46.55.42	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

09-10-2016-04:04:06 to 09-10-2016-05:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.169.7.223	United States	147.237.76.30	himush.idf.i	Unauthorized Method HEAD for 147.237.76.30/	Block	1
77.138.147.0	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/information.aspx	Block	1
66.249.64.245	Israel	147.237.0.34	tikshuv.idf.	Unauthorized URL Access to www.tikshuv.idf.il/templates/contactus/contactus.aspx	Block	1
87.71.34.241	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
66.249.76.2	Israel	147.237.77.243	mobile.idf.i	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
87.71.34.241	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 87.71.34.241	Block	1
66.249.79.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
157.55.39.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
68.180.229.190	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1

09-10-2016-04:04:06 to 09-10-2016-05:04:06