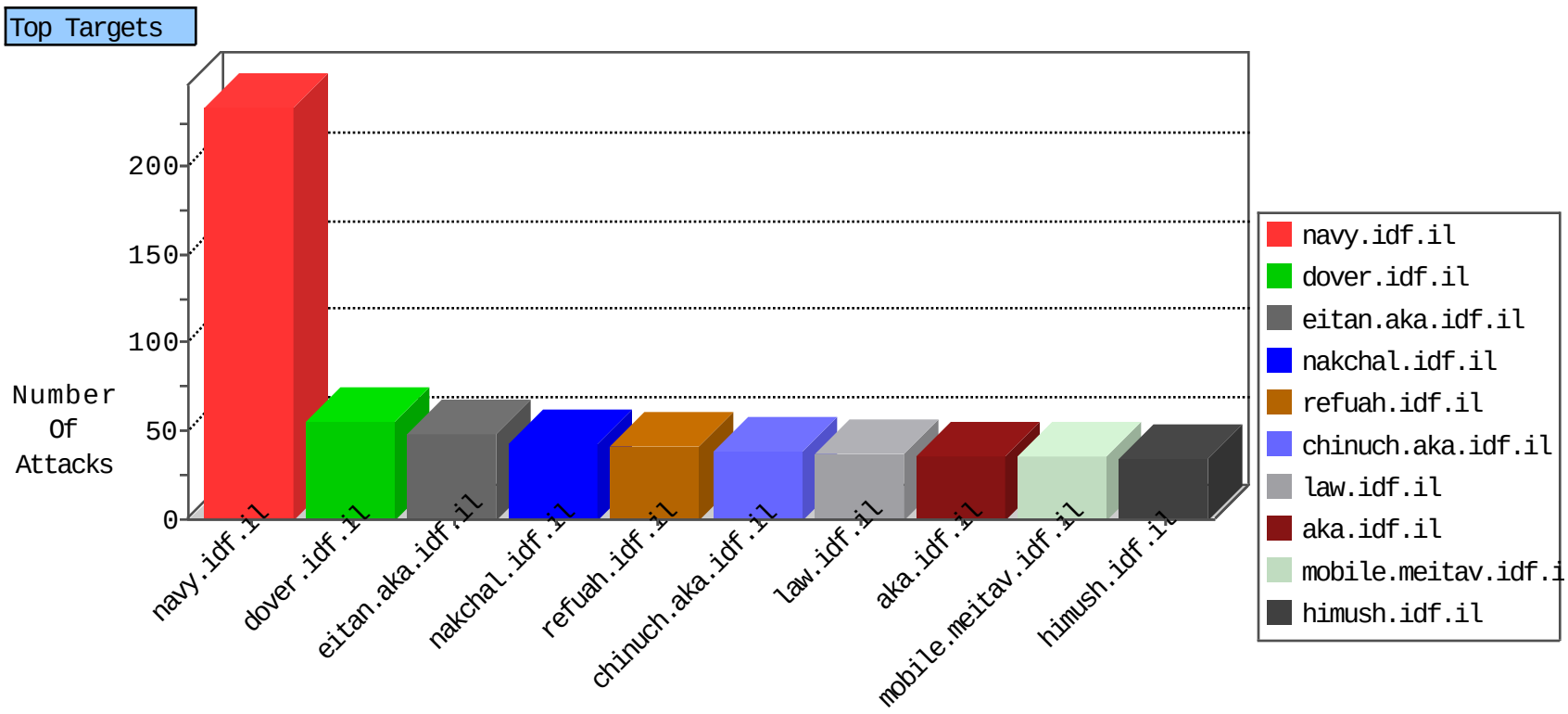
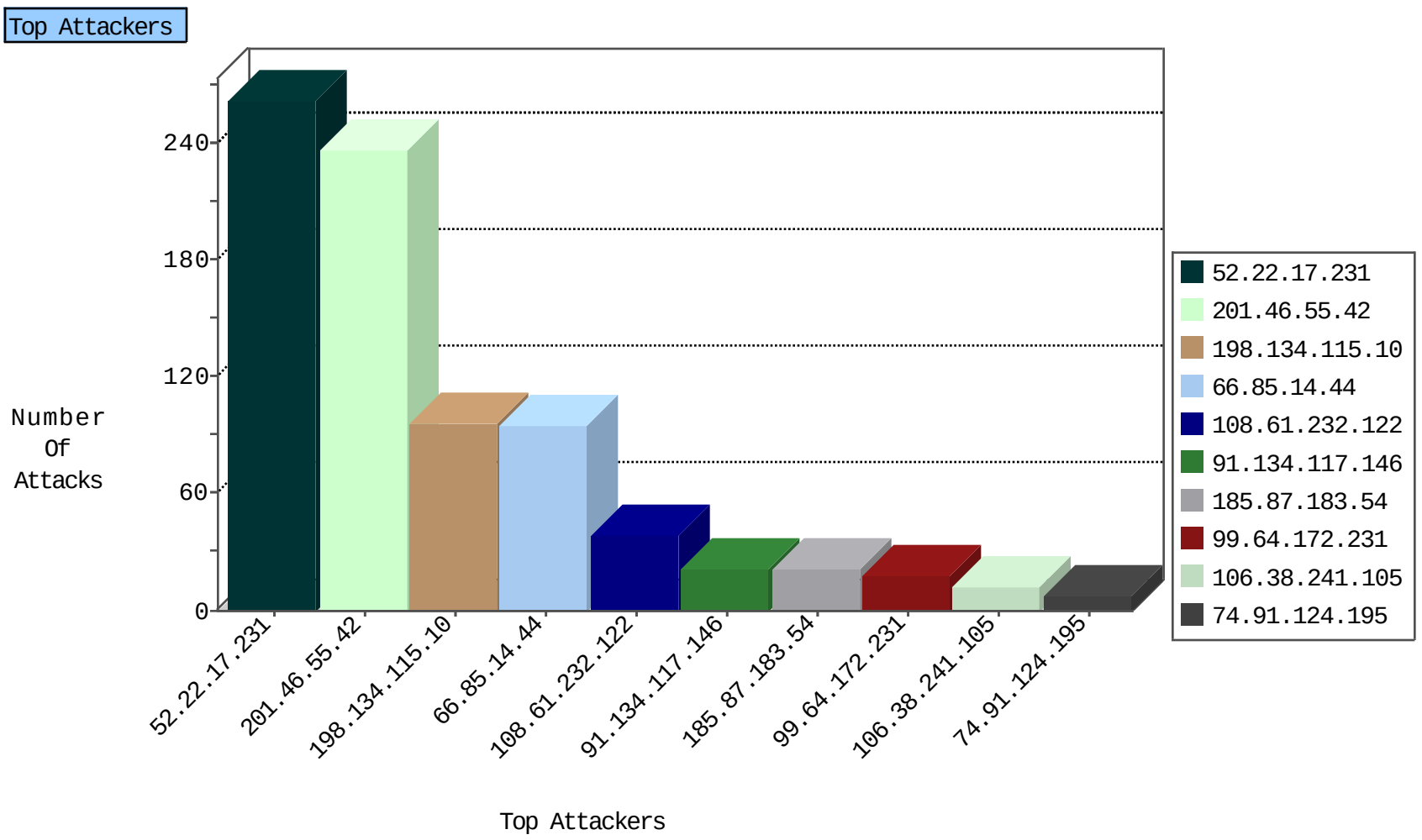
09-09-2016-02:04:00 to 09-09-2016-03:04:00

IDF Under Attack Daily Report





09-09-2016-02:04:00 to 09-09-2016-03:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.174.93.156	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
185.25.33.139	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.25.33.140	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

09-09-2016-02:04:00 to 09-09-2016-03:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
106.38.241.105	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
106.38.241.105	China	147.237.72.156	aman.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
106.38.241.105	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
106.38.241.105	China	147.237.76.200	eitan.aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
71.6.167.142	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
195.154.232.58	France	147.237.77.176	matpash.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

09-09-2016-02:04:00 to 09-09-2016-03:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
72.167.159.8	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
66.249.88.133	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
45.79.71.122	147.237.72.166	United States	aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1
163.172.129.15	147.237.76.148	United Kingdom	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
106.38.241.105	147.237.76.86	China	navy.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
91.201.236.158	147.237.77.243	Ukraine	mobile.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.155	147.237.72.217	Ukraine	e.idf.il	ET SCAN NMAP -sS window 3072	1
89.248.172.103	147.237.76.148	Netherlands	gqcenter.aka.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
89.248.172.103	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.64.22	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
128.199.58.67	147.237.76.200	Netherlands	eitan.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.201.236.158	147.237.77.243	Ukraine	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.158	147.237.77.243	Ukraine	mobile.idf.il	ET SCAN NMAP -f -sS	1
91.201.236.155	147.237.72.217	Ukraine	e.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
89.248.172.103	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.172.103	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

09-09-2016-02:04:00 to 09-09-2016-03:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
108.61.232.122	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	39
66.85.14.44	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
66.85.14.44	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	21
66.85.14.44	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	20
66.85.14.44	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
52.22.17.231	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
201.46.55.42	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
52.22.17.231	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
52.22.17.231	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
201.46.55.42	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
52.22.17.231	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
52.22.17.231	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
201.46.55.42	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
52.22.17.231	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
52.22.17.231	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
52.22.17.231	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
52.22.17.231	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
52.22.17.231	United States	147.237.77.235	sviva.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
52.22.17.231	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
52.22.17.231	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
52.22.17.231	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
52.22.17.231	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
52.22.17.231	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
52.22.17.231	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
52.22.17.231	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
52.22.17.231	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
52.22.17.231	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
52.22.17.231	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
198.134.115.10	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
52.22.17.231	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
201.46.55.42	Brazil	147.237.76.200	eitan.aka.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
66.85.14.44	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	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	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
198.134.115.10	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
201.46.55.42	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
198.134.115.10	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
52.22.17.231	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
198.134.115.10	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
198.134.115.10	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
198.134.115.10	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
198.134.115.10	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
198.134.115.10	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
201.46.55.42	Brazil	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
201.46.55.42	Brazil	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
201.46.55.42	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
201.46.55.42	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
201.46.55.42	Brazil	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9

09-09-2016-02:04:00 to 09-09-2016-03:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.139.160.212	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	2
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
157.55.39.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane/	Block	1
66.102.9.22	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
68.180.230.33	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
176.13.237.155	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.64.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
191.103.200.127	Colombia	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.64.228	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	1
106.38.241.105	China	147.237.76.86	navy.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
204.79.180.162	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
157.55.39.46	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1

09-09-2016-02:04:00 to 09-09-2016-03:04:00