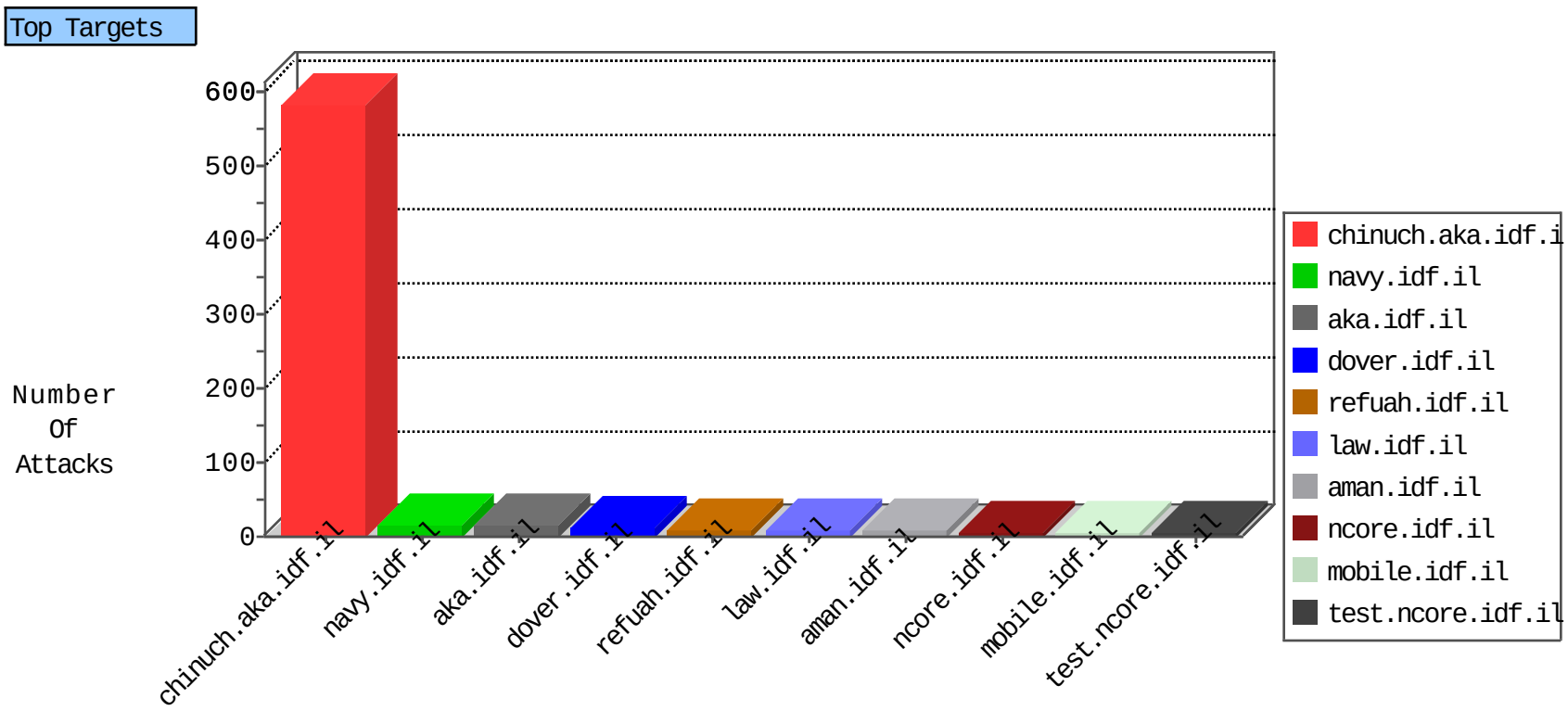
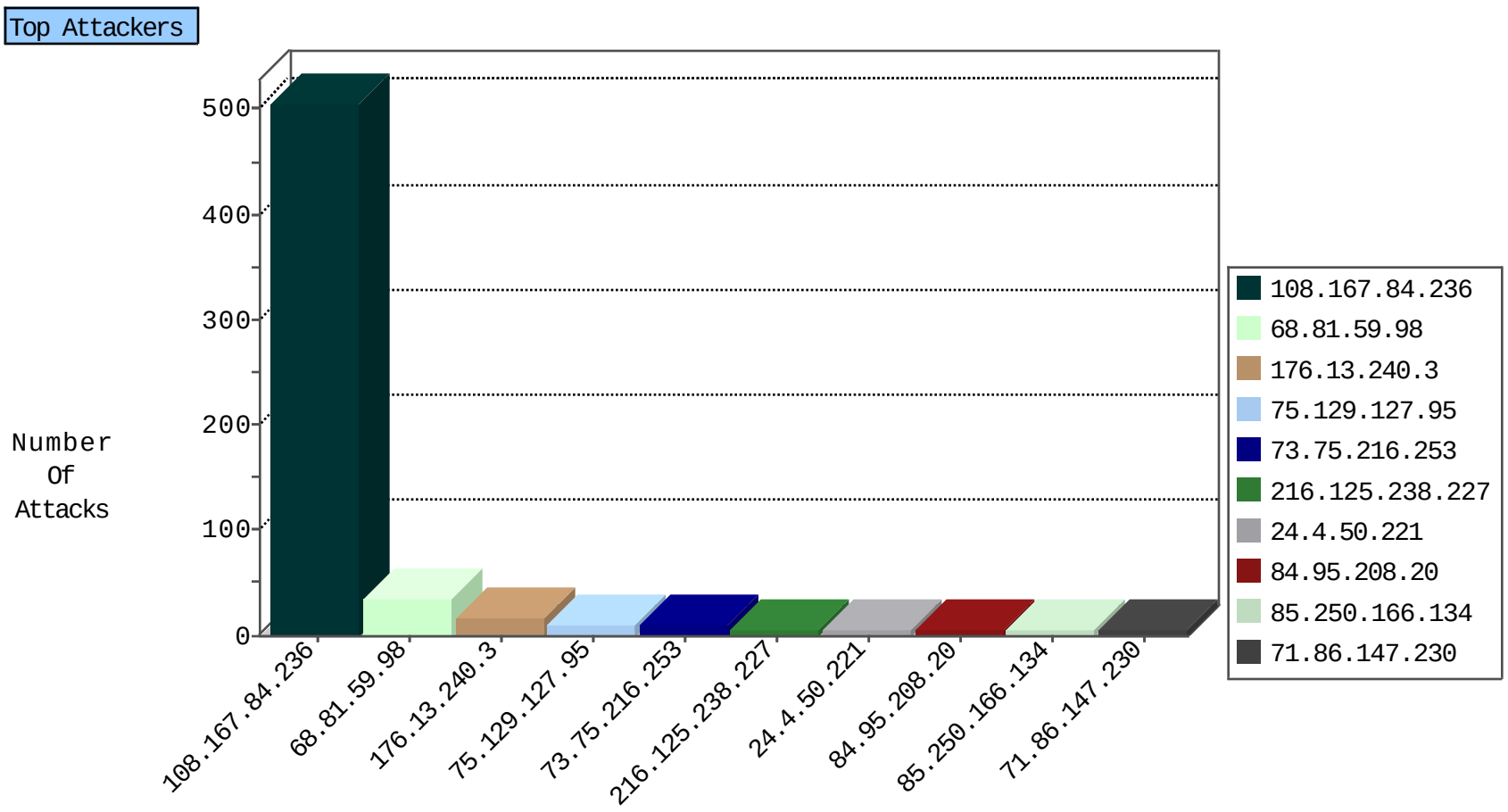
09-27-2016-05:04:00 to 09-27-2016-06:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-27-2016-05:04:00 to 09-27-2016-06:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.240.192.138	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
185.40.4.109	Russian Federation	147.237.76.86	navy.idf.il	Black List	drop	1
93.158.200.70	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	1
93.158.200.70	Netherlands	147.237.76.201	e.atal.idf.il	Black List	drop	1
93.174.94.235	Netherlands	147.237.76.176	test.ncore.idf.il	Black List	drop	1

09-27-2016-05:04:00 to 09-27-2016-06:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
83.149.126.98	Germany	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-27-2016-05:04:00 to 09-27-2016-06:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
179.43.141.198	147.237.76.176	Switzerland	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.0.200	United Kingdom	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.50	147.237.76.177	Ukraine	ncore.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
220.231.195.122	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
210.212.207.80	147.237.76.177	India	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.144.18	147.237.76.34	Switzerland	yohalan.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
149.255.108.192	147.237.77.243	United Kingdom	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
54.144.119.103	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
220.231.195.122	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -f -sS	1
179.43.144.18	147.237.77.19	Switzerland	law-forum.idf.il	ET SCAN Potential SSH Scan	1

09-27-2016-05:04:00 to 09-27-2016-06:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
108.167.84.236	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	505
68.81.59.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
176.13.240.3	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
216.125.238.227	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
85.250.166.134	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.240.3	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
75.129.127.95	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
24.4.50.221	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
75.129.127.95	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
75.129.127.95	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
176.13.239.88	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
73.75.216.253	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
43.225.194.154	India	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
109.253.217.61	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
73.75.216.253	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
73.75.216.253	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
73.75.216.253	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
75.129.127.95	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
73.75.216.253	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
109.173.32.191	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
24.4.50.221	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
89.248.174.37	Netherlands	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
184.105.247.239	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
77.124.29.54	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
74.82.47.34	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
71.86.147.230	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1
176.13.240.3	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
89.248.174.37	Netherlands	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
76.31.48.234	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
138.246.253.19	Germany	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
79.177.100.241	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
71.86.147.230	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
176.13.240.3	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
24.4.50.221	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1
93.174.93.100	Netherlands	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
76.31.48.234	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
71.86.147.230	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.165	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
79.177.100.241	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
24.4.50.221	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
76.31.48.234	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1
74.82.47.16	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
71.86.147.230	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
141.212.122.166	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.133.249.120	Spain	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
76.31.48.234	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
74.82.47.27	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
71.86.147.230	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1

09-27-2016-05:04:00 to 09-27-2016-06:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.237.76.204	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	5
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	3
46.19.85.93	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
141.226.161.47	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/terms.aspx	Block	1
68.81.59.98	United States	147.237.76.147	chinuch.aka.idf.i	NULL Character in Method [[[#0]][[#0]][[#0]][[#19]]¦VÃÙ•e¡Ùz¼ïÑ¾Ê•÷}	Block	1
66.102.6.3	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	1
66.249.76.57	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim1/main792b.html	Block	1
157.55.39.60	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in aka.idf.il/ishurim/cityofficers/	None	1
68.81.59.98	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to 147.237.76.147/	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
68.81.59.98	United States	147.237.76.147	chinuch.aka.idf.i	Abnormally Long Request method	Block	1
180.76.15.136	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9236-he/refuah.aspx	Block	1
68.81.59.98	United States	147.237.76.147	chinuch.aka.idf.i	Unknown HTTP Request Method [[[#0]][[#0]][[#0]][[#19]]¦VÃÙ•e¡Ùz¼ïÑ¾Ê•÷} in URL	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/general/piwik.php	Block	1
68.81.59.98	United States	147.237.76.147	chinuch.aka.idf.i	Illegal Byte Code Character in Method [[[#0]][[#0]][[#0]][[#19]]¦VÃÙ•e¡Ùz¼ïÑ¾Ê•÷}	Block	1
188.165.208.29	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
69.159.50.180	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
68.81.59.98	United States	147.237.76.147	chinuch.aka.idf.i	Illegal Byte Code Character in URL	Block	1
207.46.13.6	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
83.149.126.98	Germany	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
66.249.75.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-23010-ar/dover.aspx	Block	1

09-27-2016-05:04:00 to 09-27-2016-06:04:00