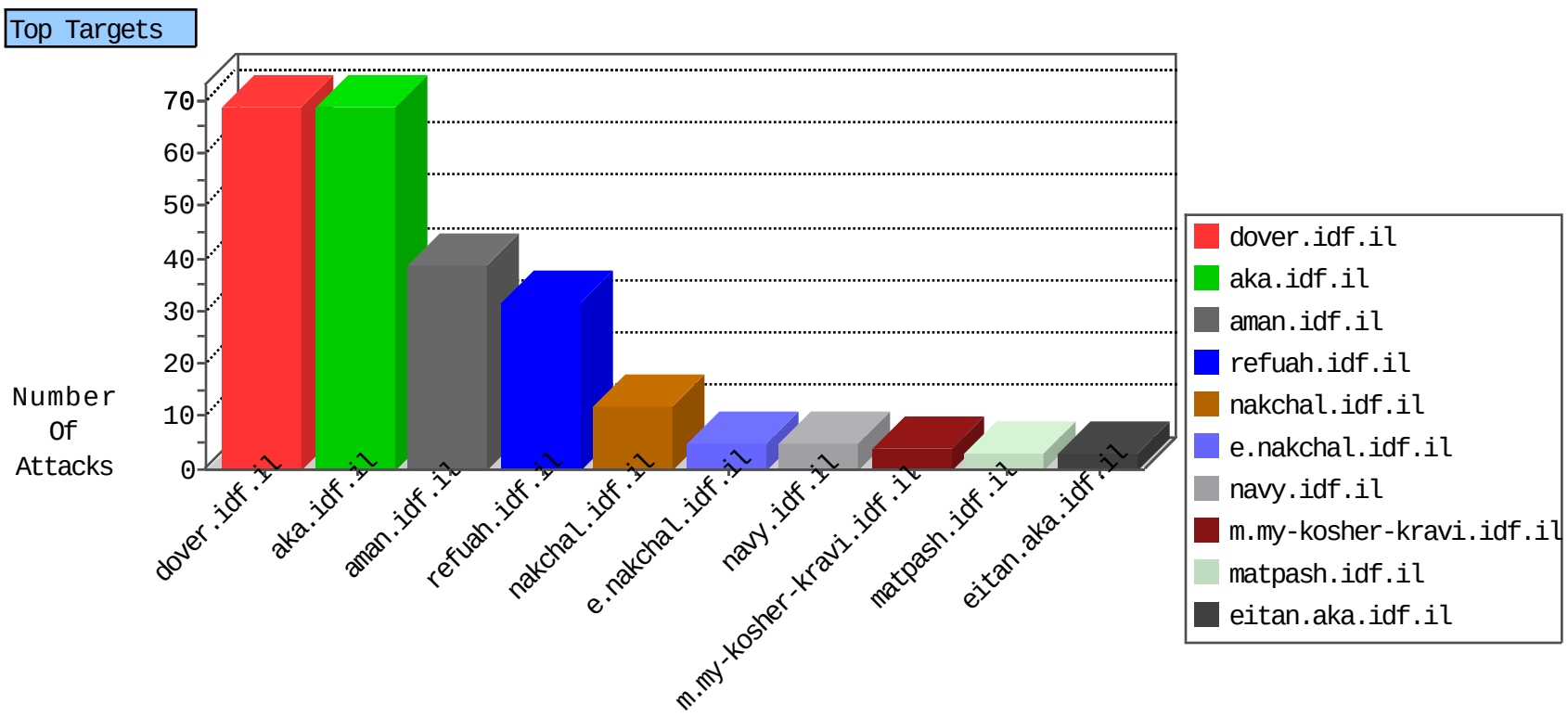
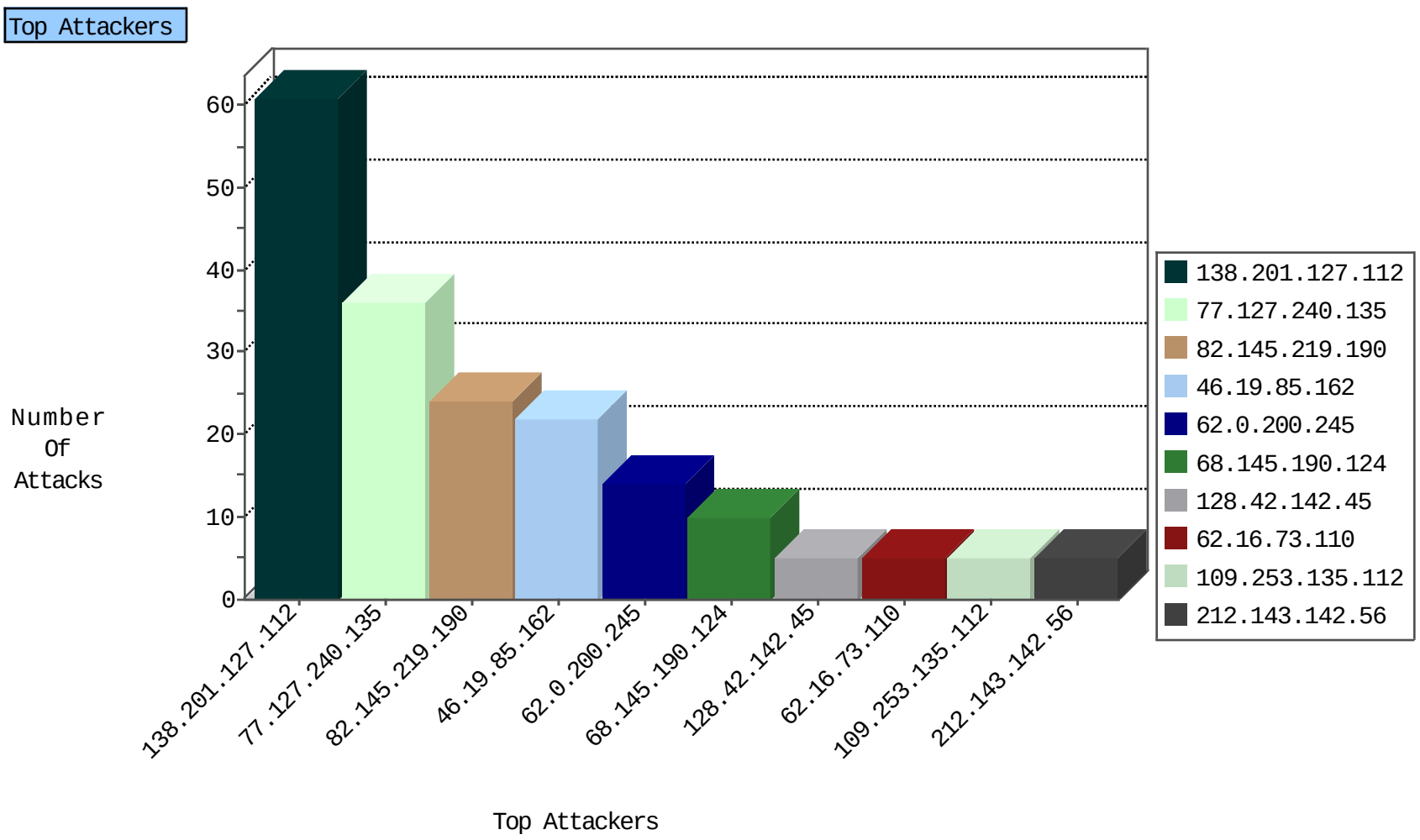
09-15-2016-04:04:02 to 09-15-2016-05:04:02

IDF Under Attack
Daily Report





09-15-2016-04:04:02 to 09-15-2016-05:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
153.90.1.35	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
139.78.141.243	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
195.113.161.82	Czech Republic	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-15-2016-04:04:02 to 09-15-2016-05:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
138.201.127.112	Germany	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	32
138.201.127.112	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	24
138.201.127.112	Germany	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
138.201.127.112	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	1
138.201.127.112	Germany	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	1
138.201.127.112	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	1

09-15-2016-04:04:02 to 09-15-2016-05:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
94.102.48.195	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.50	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
177.200.192.51	147.237.76.199	Brazil	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
163.172.129.15	147.237.0.200	United Kingdom	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
46.227.67.158	147.237.77.235	Sweden	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
177.200.192.51	147.237.76.199	Brazil	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
177.200.192.51	147.237.76.199	Brazil	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1

09-15-2016-04:04:02 to 09-15-2016-05:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
82.145.219.190	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	24
62.0.200.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
77.127.240.135	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
77.127.240.135	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
77.127.240.135	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.127.240.135	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
68.145.190.124	Canada	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.162	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.162	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.135.112	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
157.55.39.0	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
62.16.73.110	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
68.145.190.124	Canada	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
62.16.73.110	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
186.128.204.113	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
64.246.178.34	United States	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	2
2.86.129.212	Greece	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
180.97.106.162	China	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
141.212.122.163	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.47	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
208.54.83.165	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
2.86.129.212	Greece	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
180.97.106.37	China	147.237.76.39	mobile.meitav.idf.il	drop	SAM rule	drop	1
184.105.139.99	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.173	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
37.26.149.157	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.37	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
106.186.113.169	Japan	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
68.145.190.124	Canada	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.32.179.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.174	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.218.206.76	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
42.153.40.7	Malaysia	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
180.97.106.37	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
68.145.190.124	Canada	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
218.22.211.69	China	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
180.97.106.162	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
46.19.85.6	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.162	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
68.145.190.124	Canada	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
201.141.13.100	Mexico	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.37	China	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1

09-15-2016-04:04:02 to 09-15-2016-05:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
74.6.53.160	United States	147.237.76.200	eitan.aka.idf.i	Unauthorized URL Access to eitan.aka.idf.il/wp-admin/	Block	1
157.55.39.196	United States	147.237.72.166	aka.idf.il	Abnormally Long Request URL	Block	1
66.249.64.12	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1

09-15-2016-04:04:02 to 09-15-2016-05:04:02