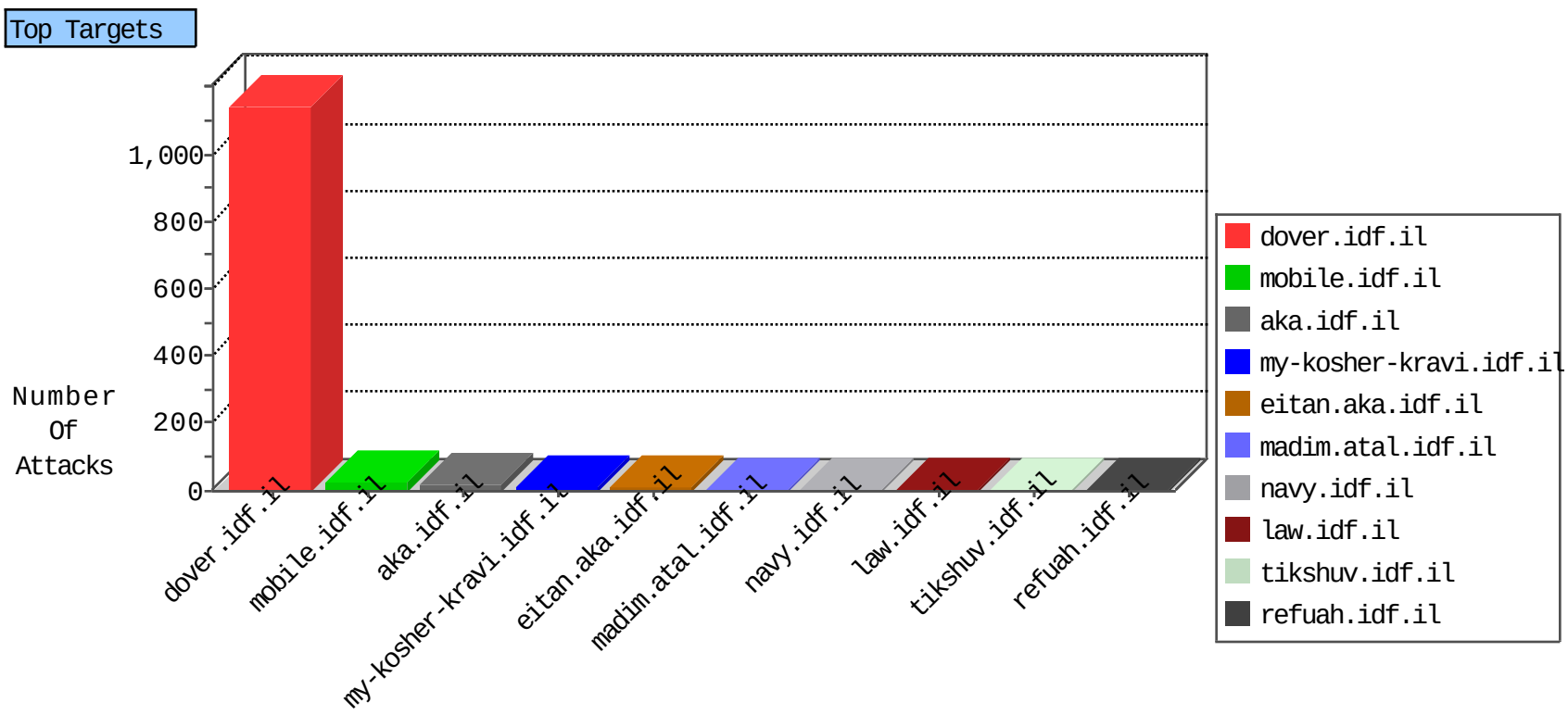
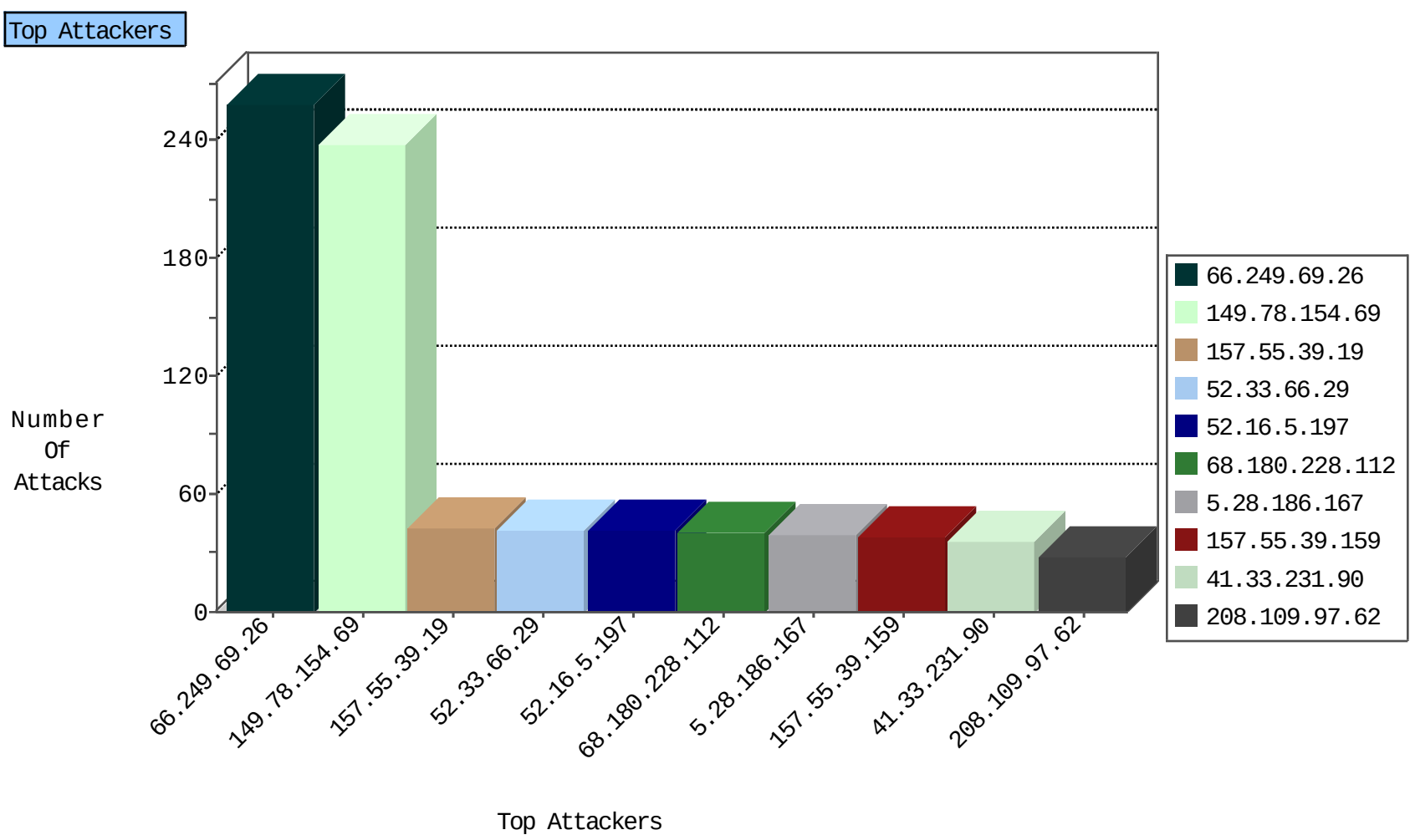
02-14-2016-05:04:04 to 02-14-2016-06:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-14-2016-05:04:04 to 02-14-2016-06:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	2
40.76.48.99	United States	147.237.76.202	e.halag.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

02-14-2016-05:04:04 to 02-14-2016-06:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
210.1.218.60	Australia	147.237.77.216	dover.idf.i	C008: HTTP: Xenu UserAgent	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
115.42.137.250	Singapore	147.237.77.216	dover.idf.i	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1

02-14-2016-05:04:04 to 02-14-2016-06:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
69.197.145.242	147.237.77.74	United States	law.idf.il	ET SCAN Potential SSH Scan	1
40.76.48.99	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
40.76.48.99	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
40.76.48.99	147.237.72.156	United States	aman.idf.il	ET SCAN Potential SSH Scan	1
201.166.227.153	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
40.76.48.99	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
177.240.72.198	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
40.76.48.99	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
116.94.50.156	147.237.0.34	Japan	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.193	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
69.197.145.242	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
62.8.75.143	147.237.76.31	Kenya	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
40.76.48.99	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
40.76.48.99	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
40.76.48.99	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
177.240.72.198	147.237.77.234	Mexico	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
40.76.48.99	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
159.122.252.59	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1

02-14-2016-05:04:04 to 02-14-2016-06:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
37.26.149.237	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
62.219.226.71	Israel	147.237.0.16	my-kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
208.109.97.62	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
157.55.12.76	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.78.223	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.221.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.28.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.235.62	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.1.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
40.77.167.75	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
75.126.221.55	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
75.126.221.55	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
199.30.25.56	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
216.218.206.118	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.106	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
203.133.168.41	Korea, Republic of	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.26	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.223	United States	147.237.0.35	akaws.idf.il	drop		drop	1
67.248.53.49	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.39	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.52	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.120.240.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
93.113.125.11	Romania	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.23	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.78	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.106	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.59	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
93.113.125.11	Romania	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.23	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	257
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	236
157.55.39.19	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	43
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	42
52.33.66.29	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	42
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	40
5.28.186.167	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	39
157.55.39.159	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	38
40.77.167.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
192.249.66.247	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	22
203.133.170.12	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	22
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
85.65.100.162	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
2.52.163.249	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
45.35.64.142		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
176.13.5.100	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
70.161.138.95	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
77.125.87.167	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
50.154.222.6	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
212.143.134.129	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
185.120.126.73		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
5.102.254.217	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
54.167.102.69	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
80.246.133.125	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	5
2.54.160.206	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
84.109.152.65	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
2.54.26.250	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
62.219.226.71	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
24.9.247.232	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
82.166.112.120	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
2.54.5.205	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
104.131.226.73	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
131.253.25.153	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
176.13.19.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
208.95.16.221	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
128.242.249.11	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
109.253.129.139	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.113	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
165.91.12.188	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
5.28.171.202	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
64.236.82.2	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
46.116.206.66	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
208.69.40.101	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
31.168.182.67	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
195.60.232.57	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2

02-14-2016-05:04:04 to 02-14-2016-06:04:04