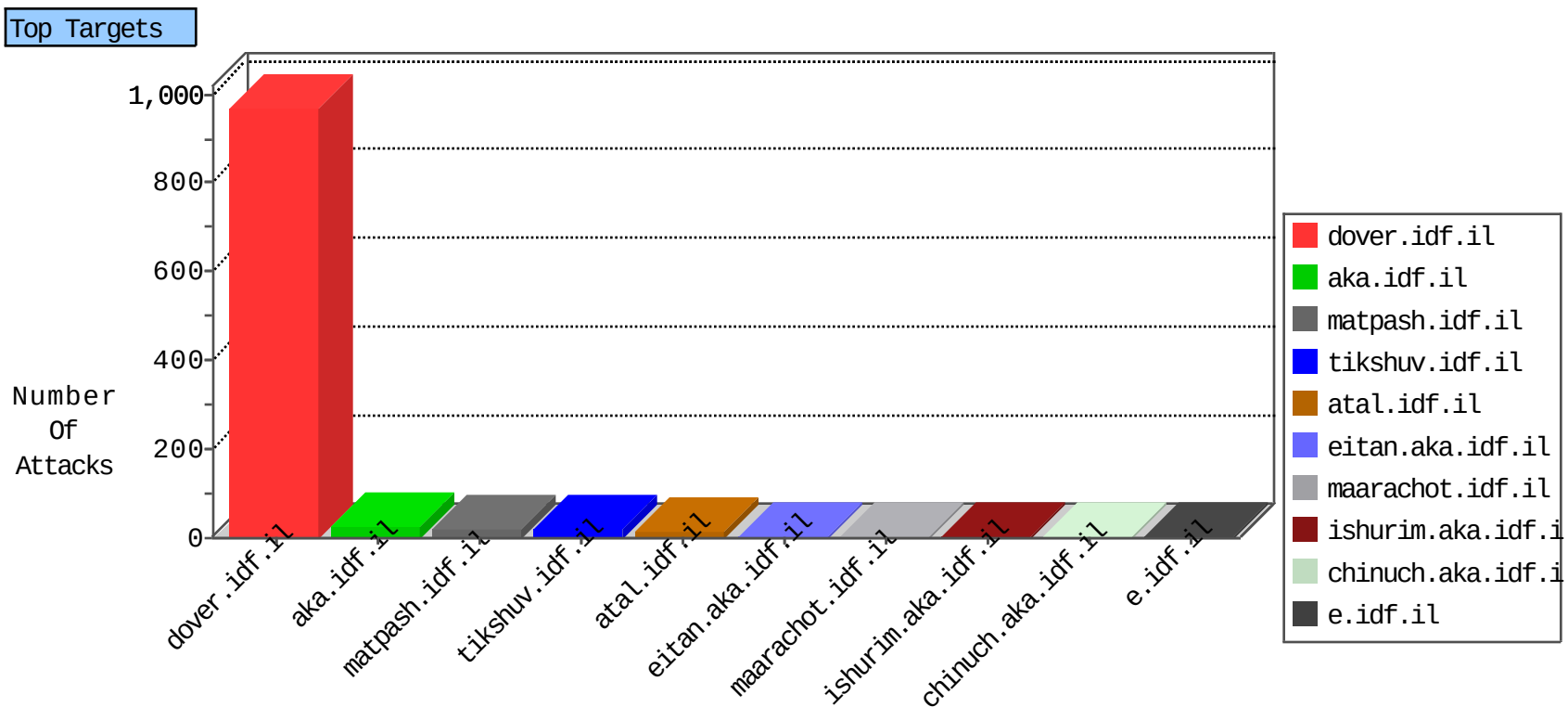
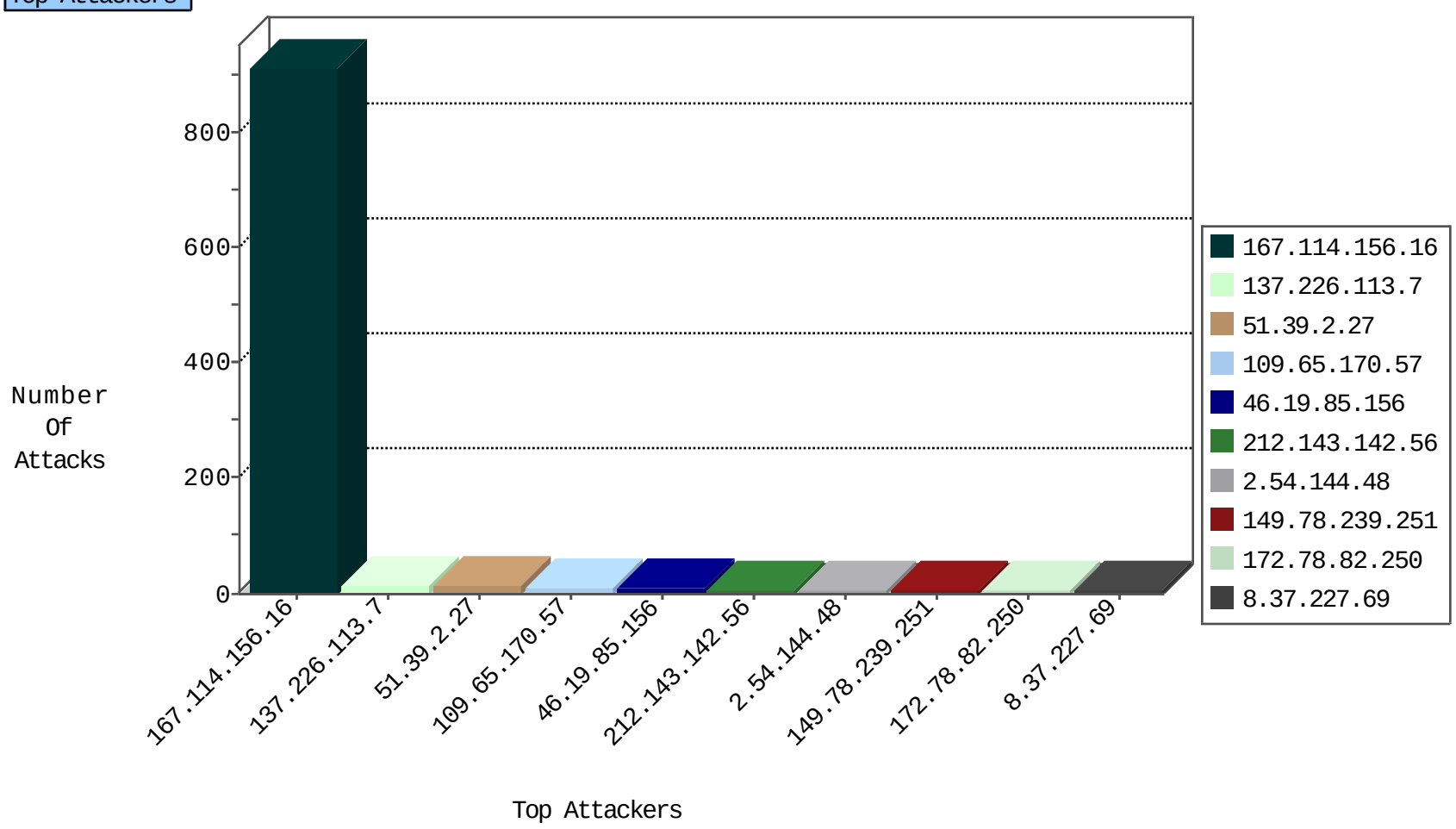
03-11-2016-01:07:47 to 03-11-2016-02:07:47

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-11-2016-01:07:47 to 03-11-2016-02:07:47

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4034
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	6
50.206.89.77	United States	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

03-11-2016-01:07:47 to 03-11-2016-02:07:47

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.170.57	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
149.78.239.251	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
109.65.93.132	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
144.76.29.162	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-11-2016-01:07:47 to 03-11-2016-02:07:47

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
93.189.26.18	147.237.8.27	Austria	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
186.113.57.238	147.237.76.31	Colombia	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
184.80.10.136	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
165.215.209.15	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
104.219.238.10	147.237.76.196		e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.76.42	Ukraine	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.76.147	Sweden	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
184.80.10.136	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
184.80.10.136	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -f -sS	1
159.122.220.109	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1

03-11-2016-01:07:47 to 03-11-2016-02:07:47

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
46.19.85.156	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.54.144.48	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
172.78.82.250		147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	5
8.37.227.68	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	4
109.201.154.151	Netherlands	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
149.78.241.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.138.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
137.226.113.7	Germany	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	3
137.226.113.7	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	3
80.246.136.58	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
137.226.113.7	Germany	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
137.226.113.7	Germany	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	3
137.226.113.7	Germany	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
204.137.241.19	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.93.26	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
51.39.2.27	United Kingdom	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
51.39.2.27	United Kingdom	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
51.39.2.27	United Kingdom	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
51.39.2.27	United Kingdom	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
51.39.2.27	United Kingdom	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
51.39.2.27	United Kingdom	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
141.212.122.139	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.94	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
176.13.1.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.215	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.129	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.88	United States	147.237.0.35	akaws.idf.il	drop		drop	1
210.186.248.71	Malaysia	147.237.77.233	atal.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
159.226.95.66	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.143	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.94	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.13.1.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
94.230.93.108	Israel	147.237.76.39	mobile.meitav.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.216	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.134	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.88	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.211	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.108.201.8	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.95	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.22.131.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.85	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.217	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

03-11-2016-01:07:47 to 03-11-2016-02:07:47

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.182.24	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
46.254.21.136	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.254.21.136	Block	3
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1129-he/dover.aspx	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2110-he/cogat.aspx	Block	1
52.30.171.229	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to /	Block	1
192.235.247.138	Canada	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.65.188	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
37.8.47.22	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17968-he/dover.aspx<span style='font-family:tahoma	Block	1
54.244.22.103	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
195.218.167.234	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
37.26.148.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
116.86.160.61	Singapore	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.119	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
195.218.167.234	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1393-en/dover.aspx	Block	1
66.249.74.104	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/4/112334.pdf	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/pazan_in_pictures/kkkkkkk=7f4d68a4kkkkkkk_7f4d68a4	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
195.218.167.234	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1393-en/dover.aspx	Block	1
66.249.74.106	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/6/111516.pdf	Block	1
46.254.21.136	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
185.25.148.240	Poland	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	1
66.249.65.181	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-9067-he/atal.aspx	Block	1

03-11-2016-01:07:47 to 03-11-2016-02:07:47