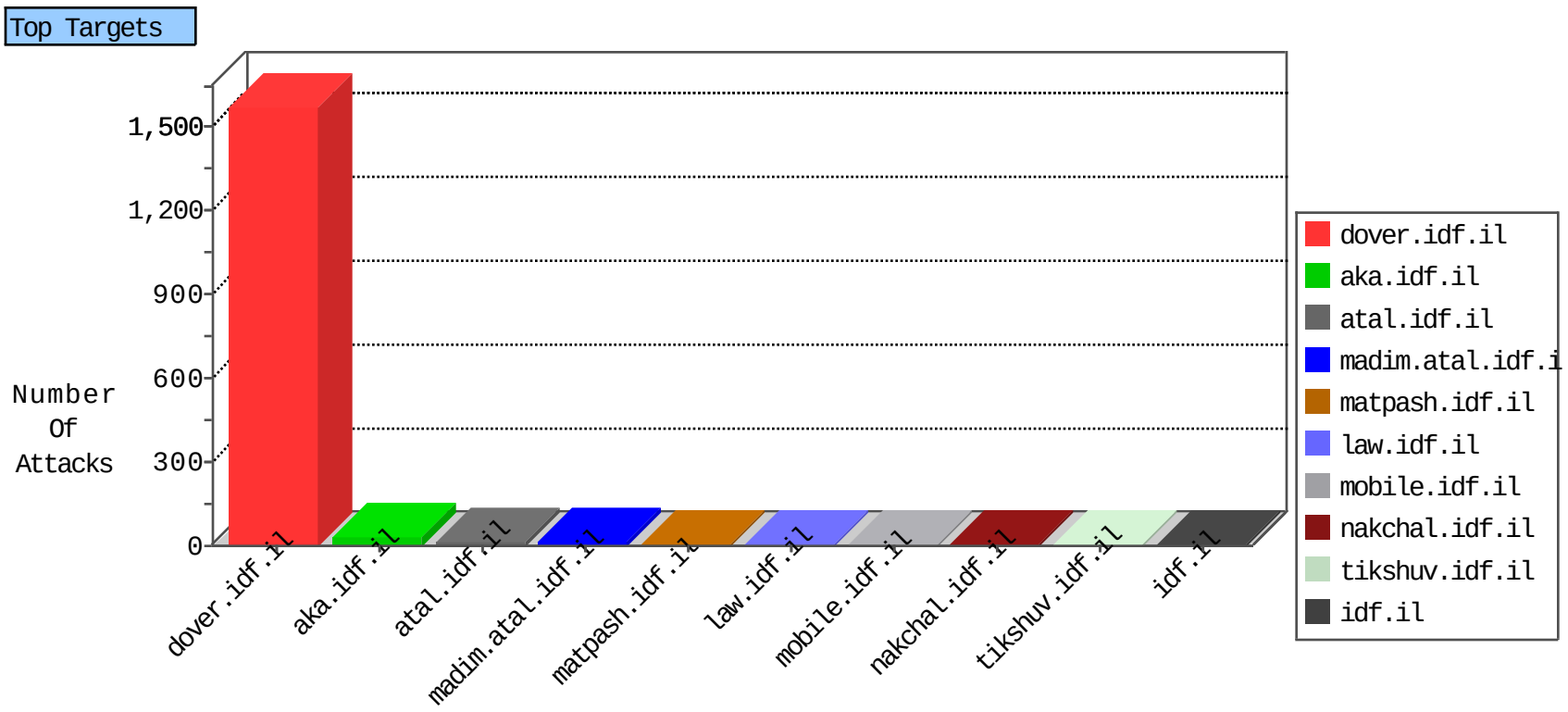
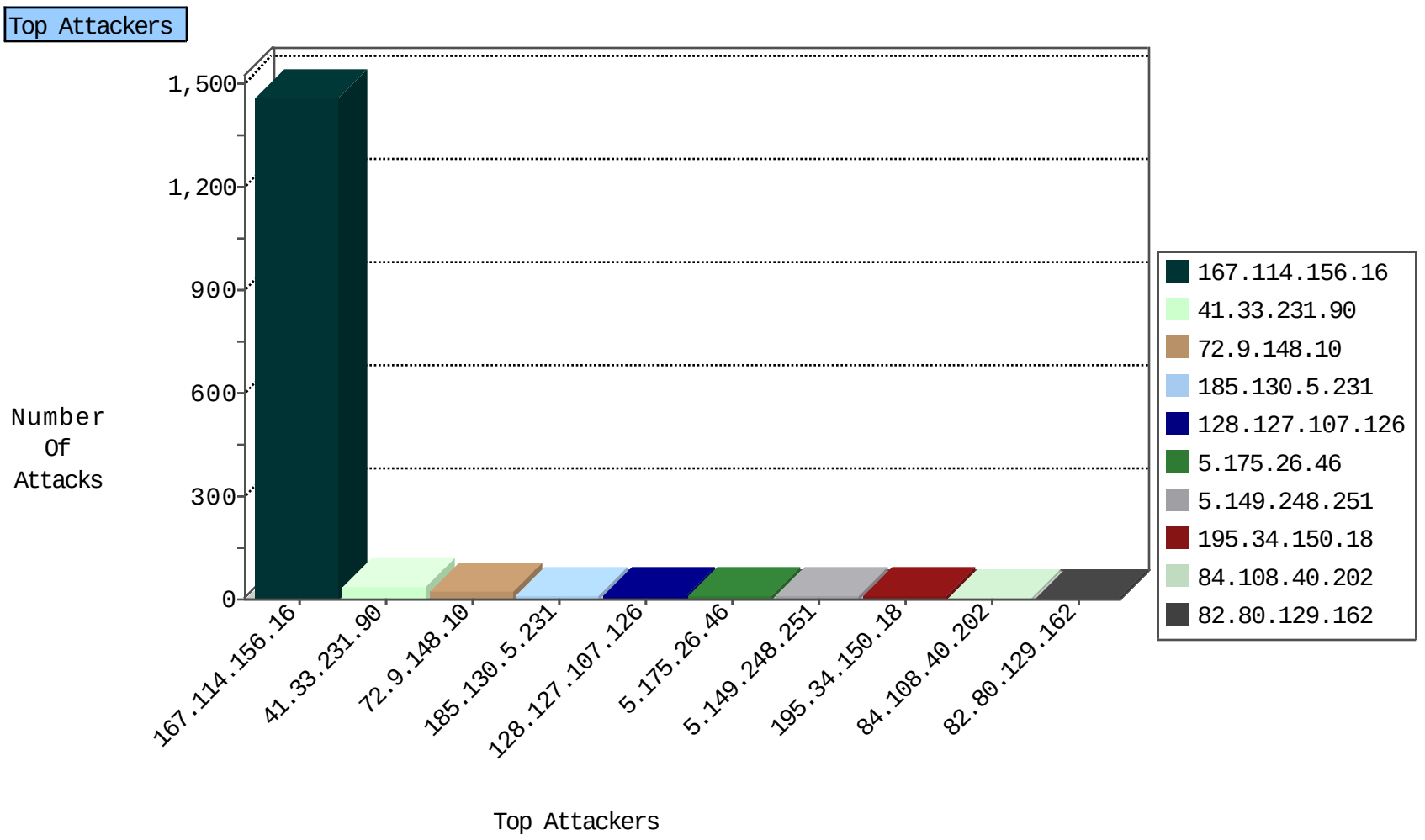
01-02-2016-07:04:01 to 01-02-2016-08:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-02-2016-07:04:01 to 01-02-2016-08:04:01

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	3167
66.249.78.153	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1134

01-02-2016-07:04:01 to 01-02-2016-08:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.130.5.224		147.237.76.147	chinuch.aka.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1

01-02-2016-07:04:01 to 01-02-2016-08:04:01

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
192.186.95.178	147.237.77.170	Canada	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
118.68.179.139	147.237.76.30	Vietnam	himush.idf.il	ET SCAN NMAP -sS window 4096	1
93.189.26.18	147.237.76.176	Austria	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
5.149.248.251	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
5.149.248.251	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
195.142.117.226	147.237.0.19	Turkey	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
192.186.95.178	147.237.77.170	Canada	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
118.68.179.139	147.237.76.30	Vietnam	himush.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.64	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
5.149.248.251	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
201.173.44.98	147.237.0.15	Mexico	kosher-kravi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
195.142.117.226	147.237.0.19	Turkey	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1

01-02-2016-07:04:01 to 01-02-2016-08:04:01

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	35
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
84.108.40.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
82.80.129.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
128.127.107.126	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
5.175.26.46	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
106.221.131.25	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
5.175.26.46	Germany	147.237.77.74	law.idf.il	drop	SAM rule	drop	3
84.228.56.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.130.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
128.127.107.126	Netherlands	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
61.135.190.71	China	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
85.64.100.186	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
149.78.207.218	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
87.69.216.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
46.120.255.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.64.100.186	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
87.69.216.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
185.130.5.231		147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
184.105.139.102	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.72	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
93.189.26.18	Austria	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.130.5.231		147.237.76.201	e.atal.idf.il	drop	SAM rule	drop	1
5.149.248.251	Netherlands	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.130.5.231		147.237.76.30	himush.idf.il	drop	SAM rule	drop	1
79.178.20.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
149.78.207.218	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
107.3.250.210	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
195.154.194.111	France	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
5.175.26.46	Germany	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
87.69.216.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.130.5.231		147.237.76.196	e.sviva.idf.il	drop	SAM rule	drop	1
184.105.247.211	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.44	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.162	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.78	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
101.198.159.31	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.231		147.237.77.19	law-forum.idf.il	drop	SAM rule	drop	1
185.130.5.231		147.237.76.39	mobile.meitav.idf.il	drop	SAM rule	drop	1
5.149.248.251	Netherlands	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.64.248.27	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
81.7.16.13	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

01-02-2016-07:04:01 to 01-02-2016-08:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.3.144.32	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	2
71.202.42.203	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	2
79.176.54.164	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
84.228.166.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
93.172.248.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.73.219	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
46.19.85.241	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
60.191.233.174	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/login/loginform.jsp	Block	1
66.249.78.27	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
46.19.85.241	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/geut/english/main.html<hr></blockquote>	Block	1
61.135.190.69	China	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on 147.237.0.19/	Block	1
5.102.236.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.34	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
52.90.147.148	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
148.251.21.227	Germany	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 148.251.21.227	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/main/giyus/general.aspx	None	1
66.249.64.153	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.85.241	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 46.19.85.241 (Open Mode)	None	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
52.90.147.148	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19850-ar/kkkkkkk=c299a07fkkkkkkk_c299a07f	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/facts.asp	Block	1
66.249.65.22	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1876	Block	1
46.19.85.241	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 46.19.85.241 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
54.67.109.119	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
180.76.15.157	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/shared/clientscripts/{1}	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1

01-02-2016-07:04:01 to 01-02-2016-08:04:01