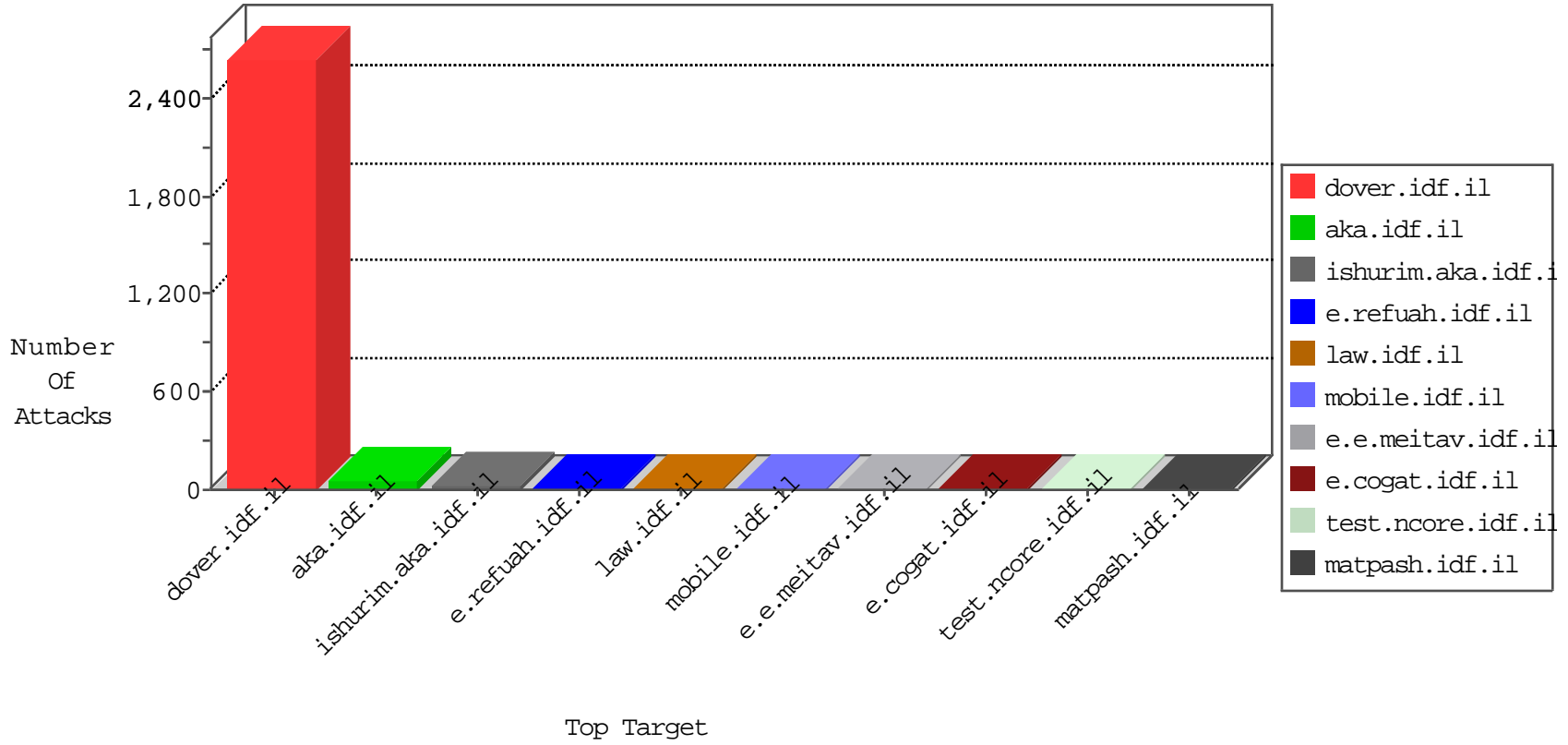


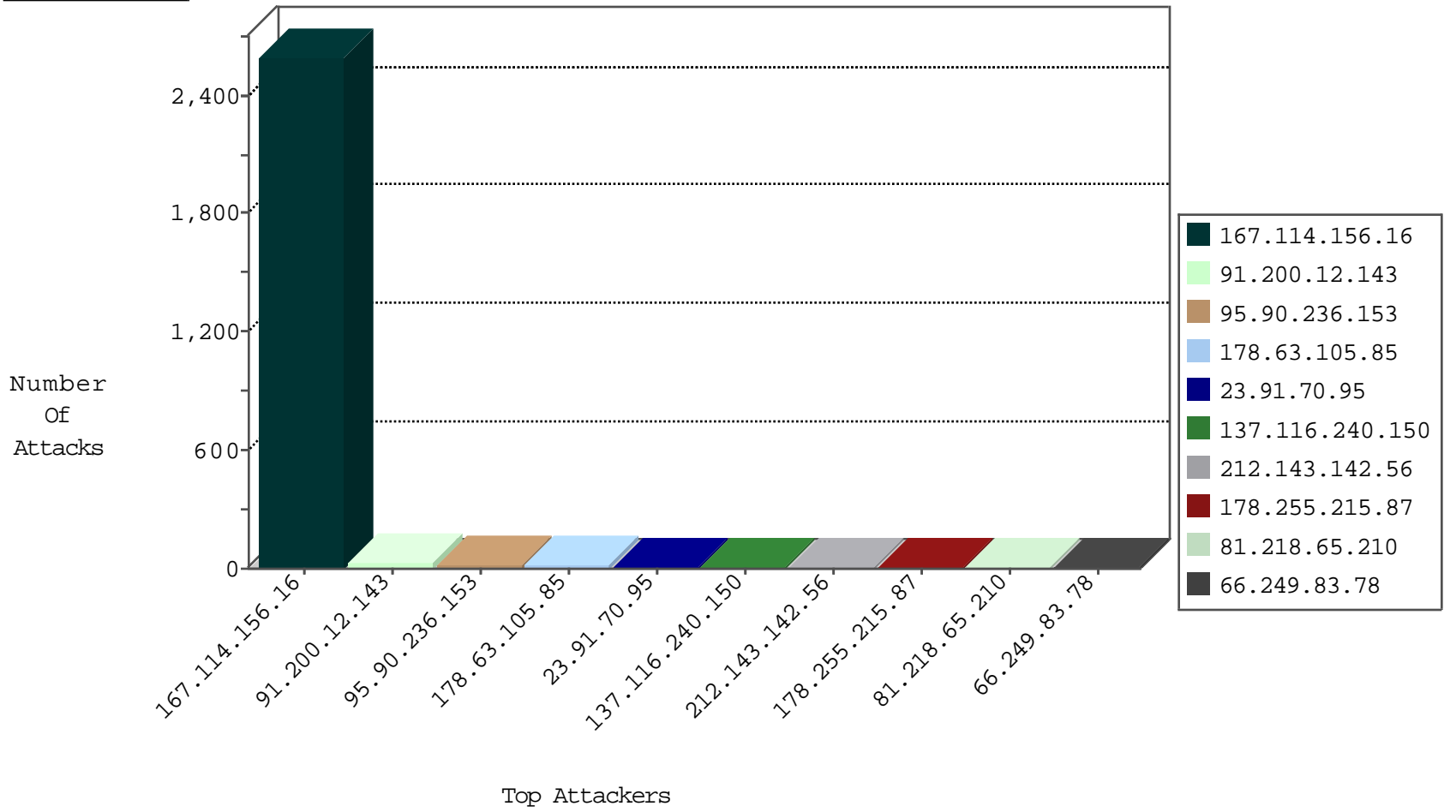
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	3362
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
66.249.78.31	Israel	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.139.104	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.104	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.112	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
23.91.70.95	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
23.91.70.95	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
188.126.77.138	147.237.76.177	Sweden	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
185.72.179.226	147.237.77.212		e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.194	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.132.187.214	147.237.77.178	Finland	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
42.116.139.91	147.237.76.199	Vietnam	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
218.24.113.2	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
188.126.77.138	147.237.77.235	Sweden	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
185.72.179.226	147.237.77.212		e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
185.72.179.226	147.237.77.212		e.dover.idf.il	ET SCAN NMAP -f -sS	1
91.201.236.114	147.237.77.216	Ukraine	dover.idf.il	ET SCAN NMAP -sS window 1024	1
79.179.201.77	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
42.116.139.91	147.237.76.199	Vietnam	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
218.24.113.2	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1

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	SYN Attack	SYN -> SYN-ACK -> RST	reject	28
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
137.116.240.150	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	5
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	5
95.90.236.153	Germany	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence		monitor	5
95.90.236.153	Germany	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.65.1.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
1.34.249.102	Taiwan	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
95.90.236.153	Germany	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence		alert	3
2.54.57.72	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
92.50.142.190	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.230	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	3
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop		drop	2
62.210.132.11	France	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	2
2.54.179.32	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
95.90.236.153	Germany	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
216.218.206.71	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.168	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.115	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.28	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.161	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
95.90.236.153	Germany	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1
216.218.206.95	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.169	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
137.116.71.170	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.199	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.35	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.162	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
95.90.236.153	Germany	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
217.132.148.124	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.7.17.171	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
62.210.254.123	France	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
159.226.95.66	China	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
201.27.203.13	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.44	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.165	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.160	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
95.90.236.153	Germany	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
74.82.47.55	United States	147.237.76.147	chinuch.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
91.200.12.143	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	12
91.200.12.143	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 91.200.12.143	Block	11
66.249.83.78	Israel	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	5
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
184.105.139.67	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
5.18.186.139	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/894-he/chinuch.aspx	Block	1
66.249.66.82	Israel	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
186.159.147.157	Costa Rica	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 186.159.147.157 (Open Mode)	None	1
68.180.228.241	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/kamlar/adv.asp	Block	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
186.159.147.157	Costa Rica	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
80.82.65.82	Netherlands	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
91.200.12.143	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus/index.php	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/gyus/general.aspx	Block	1
207.46.13.35	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/gyus/general.aspx	Block	1
86.98.1.206	United Arab Emirates	147.237.77.216	doover.idf.il	PHP Attempt	Block	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
157.55.39.44	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
208.115.113.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/html/1.asp	Block	1
86.98.1.206	United Arab Emirates	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
62.210.254.123	France	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1