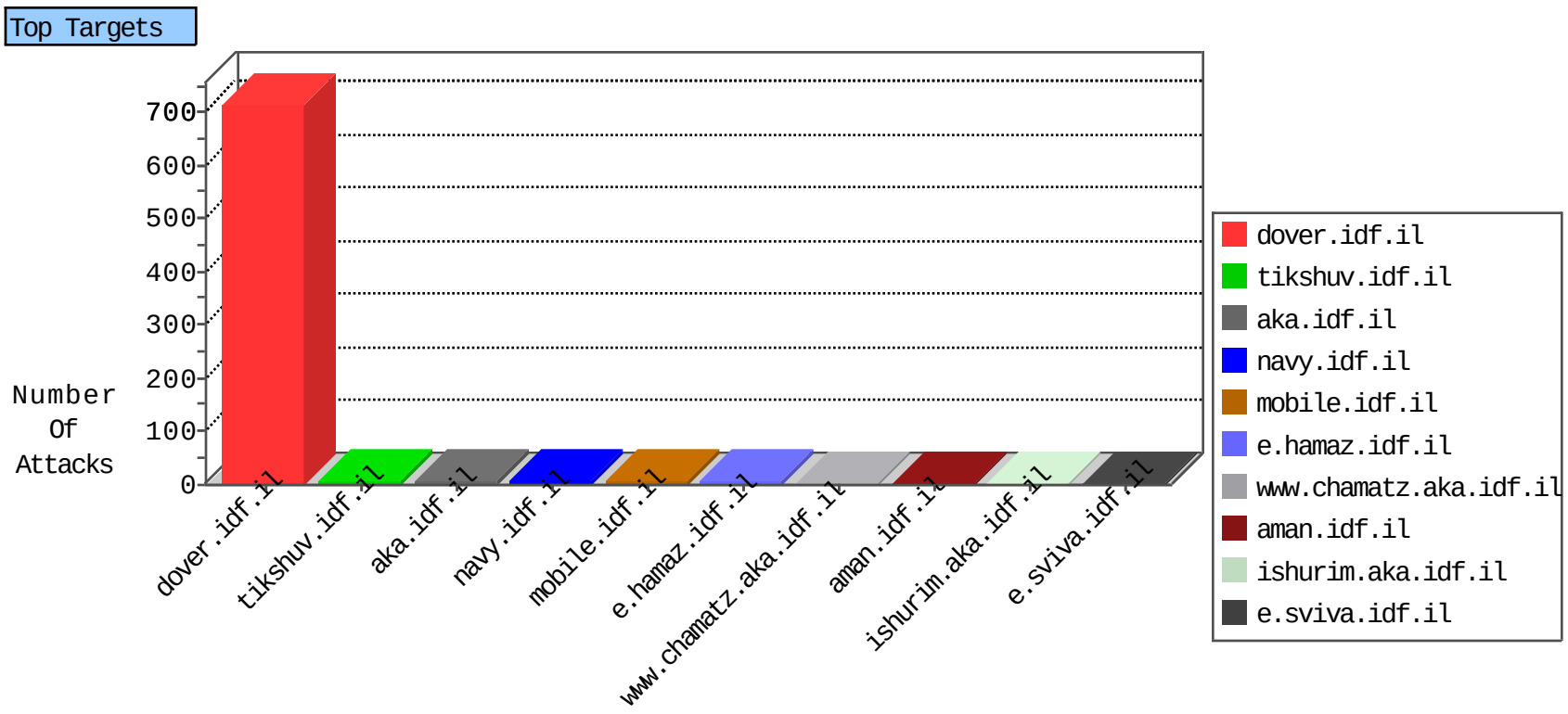
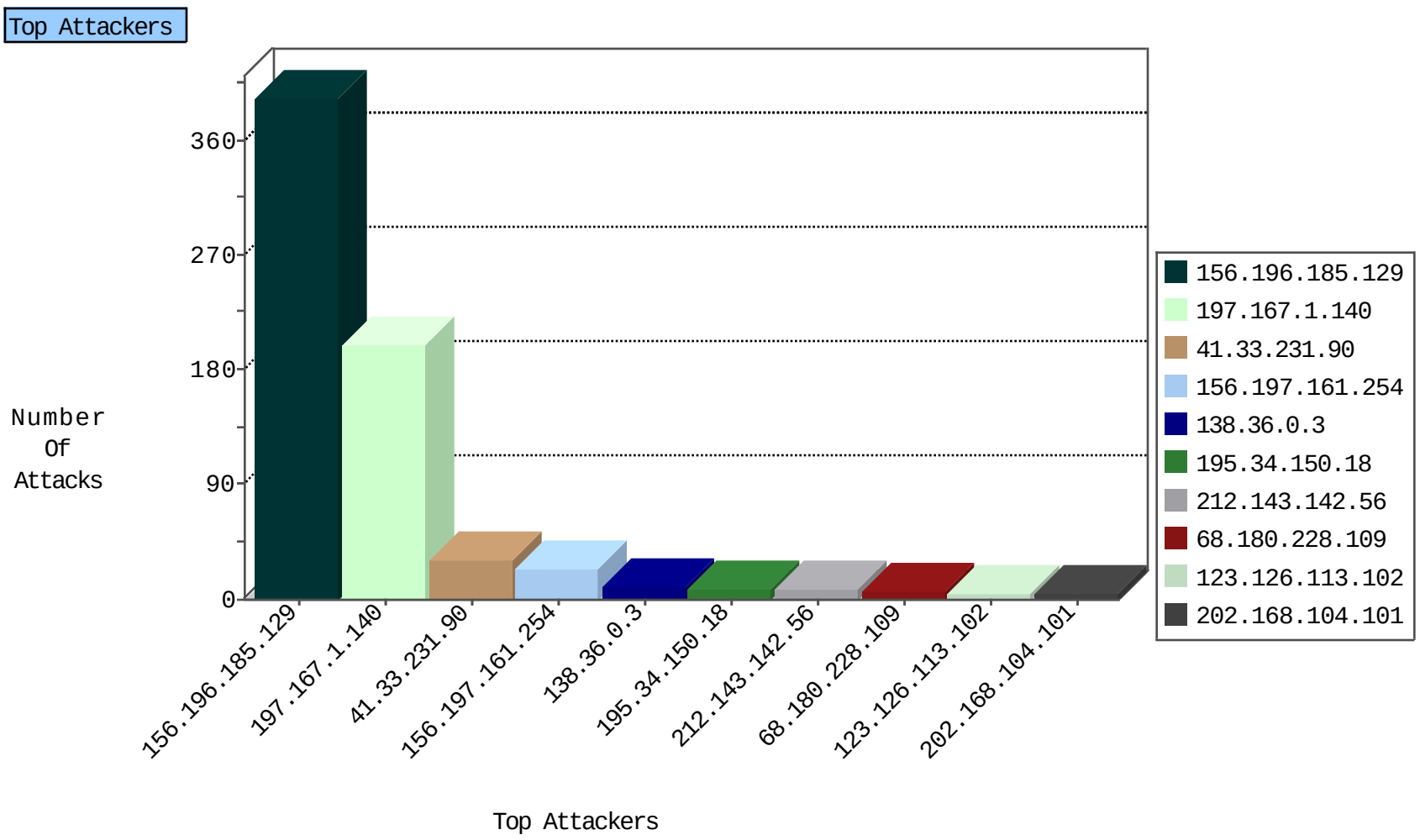
02-27-2016-03:04:03 to 02-27-2016-04:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-27-2016-03:04:03 to 02-27-2016-04:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
156.196.185.129		147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	225
156.196.185.129		147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	184
0.0.0.0		147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	182
197.167.1.140	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	133
197.167.1.140	Egypt	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	45
156.197.161.254		147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	20
156.197.161.254		147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	9
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
125.75.206.156	China	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	2
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
4.15.125.104	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
141.150.59.46	United States	147.237.72.14	dover.idf.il(old)	Block_Udp_All_Nets	drop	1

02-27-2016-03:04:03 to 02-27-2016-04:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.102	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
207.46.13.145	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
157.55.39.92	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

02-27-2016-03:04:03 to 02-27-2016-04:04:03

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
183.61.109.189	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
146.185.250.2	147.237.77.227	Russian Federation	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
104.44.133.108	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.113	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
82.200.142.180	147.237.77.205	Kazakstan	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.69.71	147.237.8.28	France	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
38.105.146.70	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
14.33.123.39	147.237.0.33	Korea, Republic of	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
146.185.250.2	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN Potential SSH Scan	1
138.36.0.3	147.237.77.234		halag.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
82.200.142.180	147.237.77.205	Kazakstan	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
62.210.142.238	147.237.76.177	France	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
45.43.226.154	147.237.76.147		chinuch.aka.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
38.105.146.70	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1

02-27-2016-03:04:03 to 02-27-2016-04:04:03

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	30
197.167.1.140	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
156.196.185.129		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
93.173.238.216	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
202.168.104.101	Australia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
66.249.79.121	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.36.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.79.119	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
98.116.130.36	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
197.167.1.140	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
109.186.58.104	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
217.69.133.230	Russian Federation	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
136.243.47.150	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
204.79.180.244	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.116	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
138.36.0.3		147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
114.112.90.54	China	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
88.200.214.8	Russian Federation	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
197.167.1.140	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
136.243.47.152	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
98.116.130.36	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
204.79.180.244	United States	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
184.105.247.251	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
138.36.0.3		147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.125.71.78	China	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
88.200.214.8	Russian Federation	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.75	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
138.36.0.3		147.237.0.35	akaws.idf.il	drop		drop	1
81.218.79.211	Israel	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
138.36.0.3		147.237.76.34	yohalan.idf.il	drop		drop	1
123.125.71.78	China	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
88.200.214.8	Russian Federation	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
64.134.243.109	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.82	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
138.36.0.3		147.237.0.200	m4u.idf.il	drop		drop	1
109.186.58.104	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.57.164.201	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
87.69.62.195	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.62.53.168	Russian Federation	147.237.0.33	idf.il	drop		drop	1
138.36.0.3		147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.126.113.102	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.88	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
138.36.0.3		147.237.8.28	e.mobile-ks.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
87.69.112.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
195.62.53.168	Russian Federation	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

02-27-2016-03:04:03 to 02-27-2016-04:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
65.55.210.84	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
80.246.133.170	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
69.63.185.116	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
173.252.115.198	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
71.227.165.148	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
201.156.161.243	Mexico	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
78.47.62.212	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
202.168.104.101	Australia	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
217.69.133.232	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/	Block	1
66.249.66.37	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
157.55.39.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

02-27-2016-03:04:03 to 02-27-2016-04:04:03