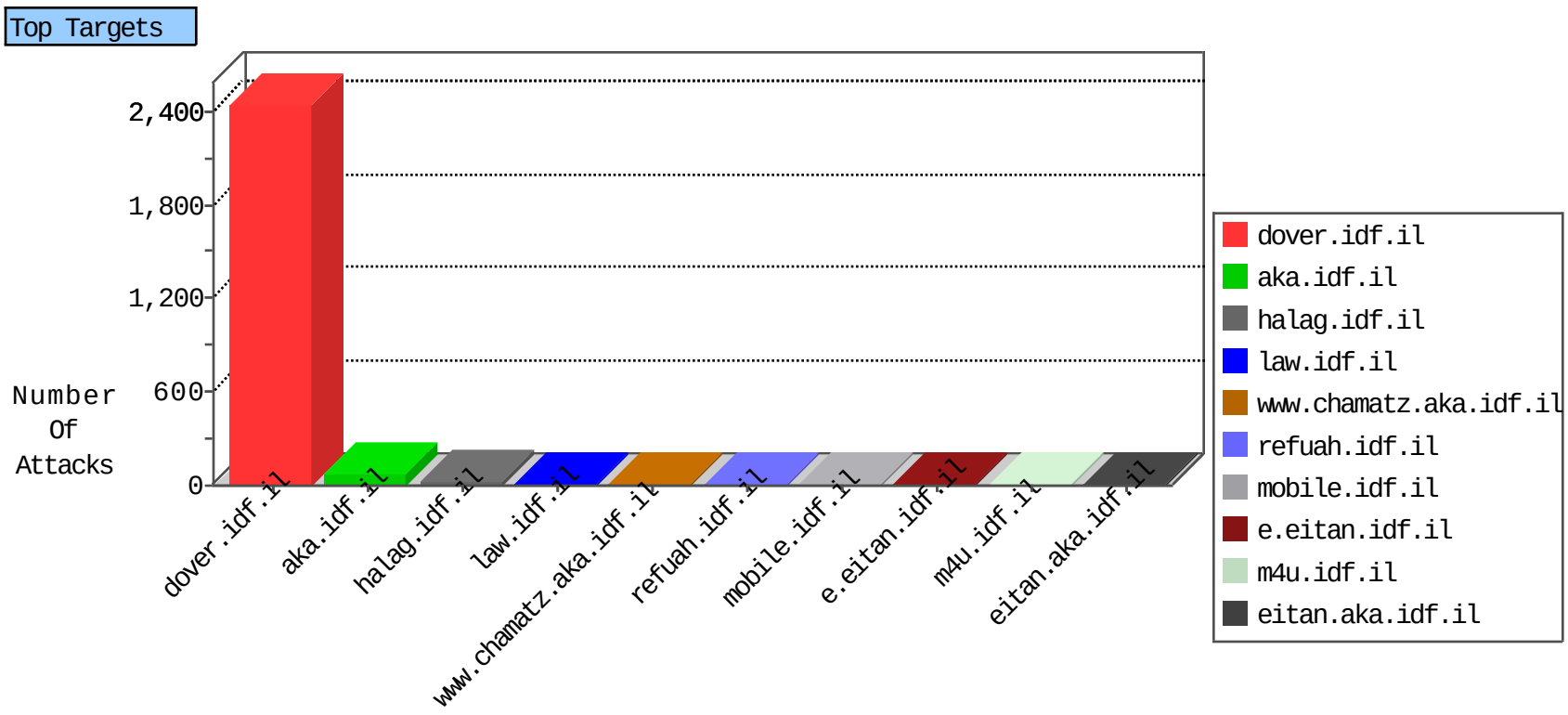
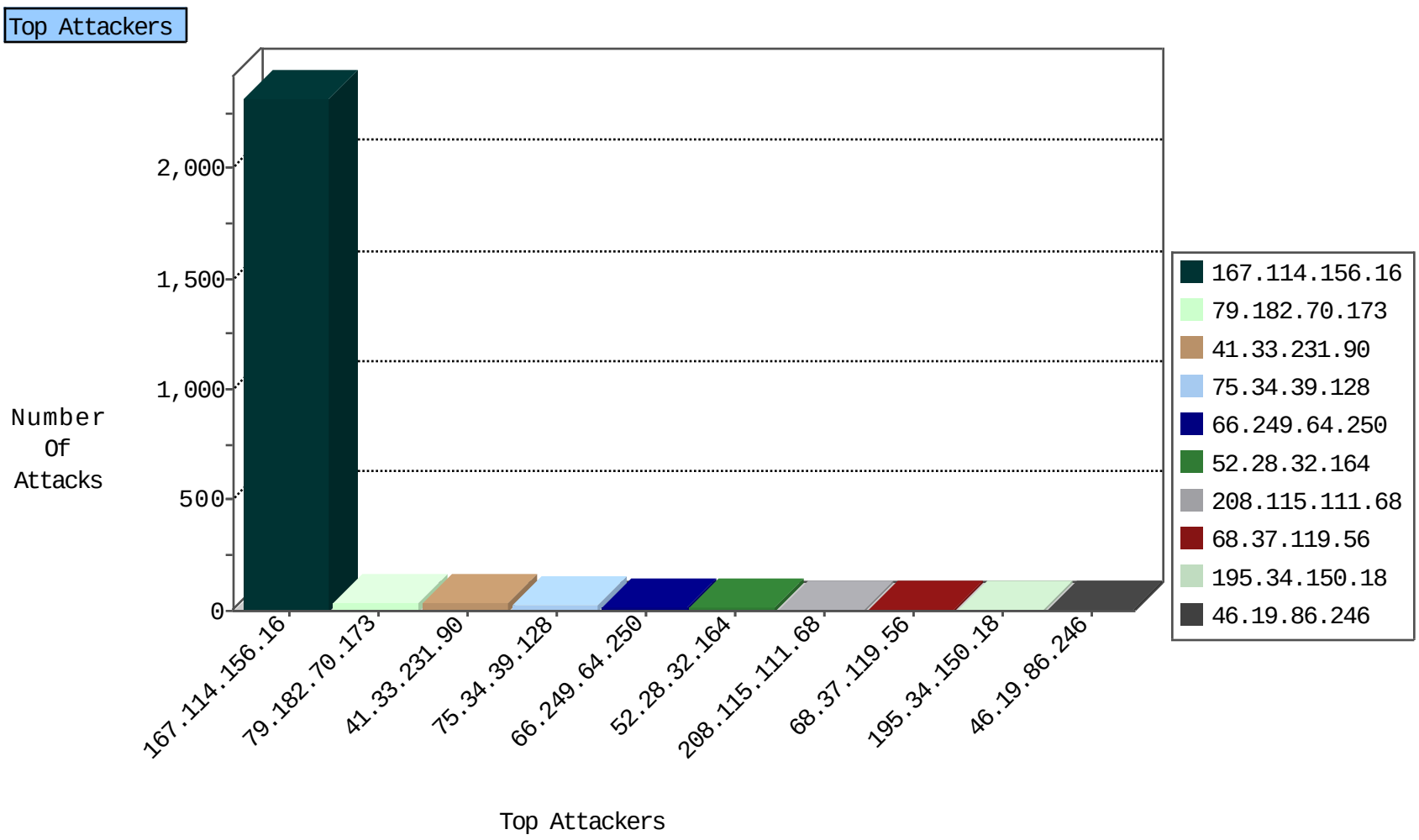
12-21-2015-03:04:05 to 12-21-2015-04:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-21-2015-03:04:05 to 12-21-2015-04:04:05

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	3445

12-21-2015-03:04:05 to 12-21-2015-04:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.147	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.152	France	147.237.0.15	kosher-kravi.idf.il	C228: HTTP: AhrefBot crawler	Block	1

12-21-2015-03:04:05 to 12-21-2015-04:04:05

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
91.201.236.114	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
40.115.58.160	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
37.143.82.50	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
168.62.238.153	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
117.31.224.80	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.77.205		prisha.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
168.62.238.153	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1

12-21-2015-03:04:05 to 12-21-2015-04:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.182.70.173	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
66.249.64.250	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
208.115.111.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	10
75.34.39.128	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
157.55.2.187	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
75.34.39.128	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
75.34.39.128	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
75.34.39.128	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
66.87.115.189	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
93.173.236.124	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
146.185.234.48	Russian Federation	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
100.127.146.3		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
75.34.39.128	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.78.216	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.246	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
75.34.39.128	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
81.169.237.146	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	2
46.19.86.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
89.248.172.147	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	2
68.37.119.56	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
81.169.237.146	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	2
213.57.207.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
68.37.119.56	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
68.37.119.56	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.69.18	Israel	147.237.0.33	idf.il	drop		drop	1
52.28.32.164	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.246	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
68.37.119.56	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
52.28.32.164	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
155.94.222.12	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
52.28.32.164	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
203.127.96.216	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
52.28.32.164	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
139.196.104.39	China	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.246	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
68.37.119.56	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
52.28.32.164	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
52.28.32.164	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
2.52.176.45	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
203.127.96.216	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

12-21-2015-03:04:05 to 12-21-2015-04:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.86.92.250	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/&sa=u&ved=0ahukewi6ooh14-vjahuiaxqkhwuuanoqfggnmaa&usg=afqjcnhcdsh5ryhkeugapxldsq7fowjwnw	Block	2
85.64.16.10	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
89.138.68.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
89.248.172.147	Netherlands	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/clientscripts.js	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	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
81.209.177.189	Europe	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
5.156.163.186	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/qar/	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.69.77	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/news/news.aspx	Block	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
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
40.77.167.89	United States	147.237.76.200	eitan.aka.idf.i	Unknown Parameter version in www.eitan.aka.idf.il/css/style.css	None	1
207.46.13.129	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
87.69.91.181	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9031-he/refuah.aspx	Block	1
46.166.190.167	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
194.150.168.79	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1

12-21-2015-03:04:05 to 12-21-2015-04:04:05