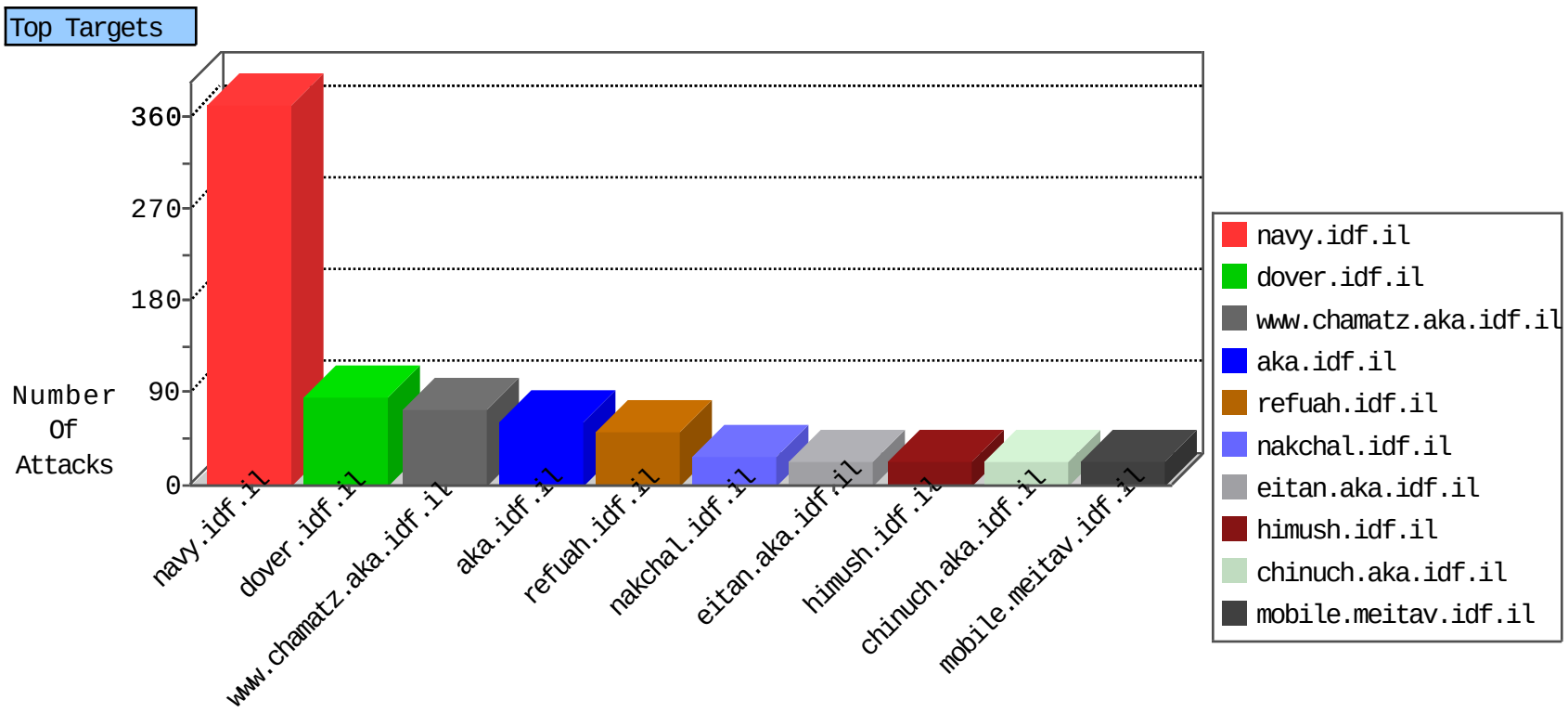
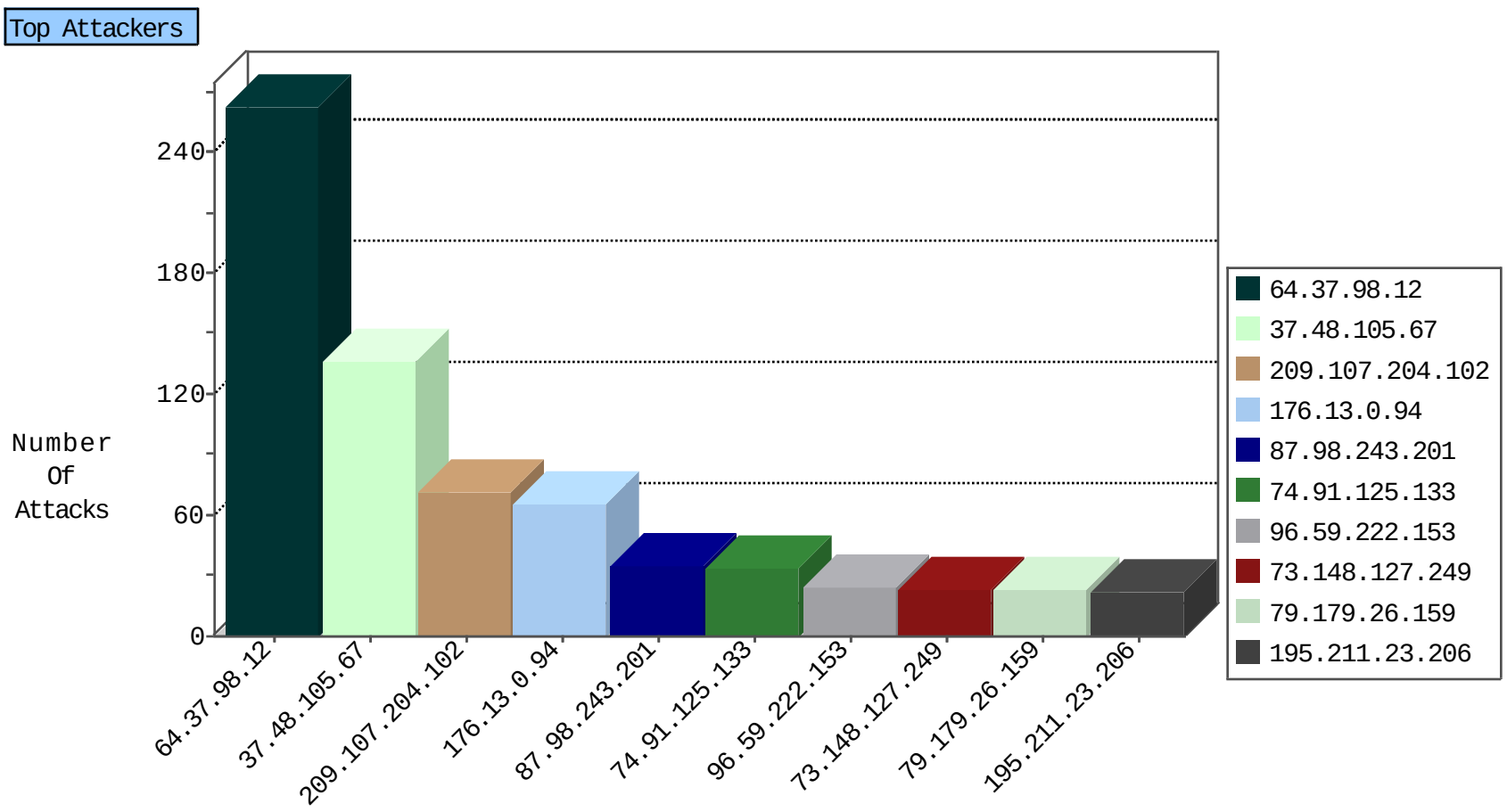
09-10-2016-01:06:42 to 09-10-2016-02:06:42

IDF Under Attack Daily Report





09-10-2016-01:06:42 to 09-10-2016-02:06:42

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
139.162.13.205	Singapore	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	1
94.177.164.99	Romania	147.237.76.31	nakchal.idf.il	Black List	drop	1
94.177.164.99	Romania	147.237.76.44	e.refuah.idf.il	Black List	drop	1
94.177.164.99	Romania	147.237.76.176	test.ncore.idf.il	Black List	drop	1

09-10-2016-01:06:42 to 09-10-2016-02:06:42

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.98	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-10-2016-01:06:42 to 09-10-2016-02:06:42

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
144.76.185.234	147.237.77.170	Germany	maarachot.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
84.93.84.77	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
45.79.103.178	147.237.0.34	United States	tikshuv.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
178.20.188.164	147.237.77.179	Jordan	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
174.37.222.106	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
144.76.172.150	147.237.77.170	Germany	maarachot.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
106.186.20.183	147.237.76.199	Japan	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.141.198	147.237.72.217	Switzerland	e.idf.il	ET SCAN Potential SSH Scan	1
178.20.188.164	147.237.77.179	Jordan	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
174.37.222.106	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
144.76.167.53	147.237.77.170	Germany	maarachot.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
93.158.203.149	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
46.161.40.17	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
23.239.31.132	147.237.72.166	United States	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.255.90.133	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
178.20.188.164	147.237.77.179	Jordan	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1

09-10-2016-01:06:42 to 09-10-2016-02:06:42

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
37.48.105.67	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	136
176.13.0.94	Israel	147.237.77.226	www.chamatz.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
64.37.98.12	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
64.37.98.12	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
64.37.98.12	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
64.37.98.12	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
96.59.222.153	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
64.37.98.12	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
64.37.98.12	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
64.37.98.12	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
64.37.98.12	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
195.211.23.206	Russian Federation	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	22
209.107.204.102	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
37.35.154.100	Spain	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
79.179.26.159	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
209.107.204.102	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	16
209.107.204.102	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	15
80.246.133.140	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
209.107.204.102	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
74.91.125.133	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	9
74.91.125.133	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.46.37.100	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
74.91.125.133	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	7
209.107.204.102	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
37.46.37.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
64.37.98.12	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
64.37.98.12	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
64.37.98.12	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
64.37.98.12	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
64.37.98.12	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
64.37.98.12	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
64.37.98.12	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
64.37.98.12	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
64.37.98.12	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
64.37.98.12	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
64.37.98.12	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
64.37.98.12	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
74.91.125.133	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
64.37.98.12	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
73.148.127.249	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
212.68.131.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
74.91.125.133	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
73.148.127.249	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
64.37.98.12	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
73.148.127.249	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
73.148.127.249	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.68.131.59	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
216.244.66.243	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

09-10-2016-01:06:42 to 09-10-2016-02:06:42

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
45.79.103.178	United States	147.237.0.34	tikshuv.idf.il	Multiple Unknown HTTP Request Method from 45.79.103.178	Block	2
85.65.190.124	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
45.79.103.178	United States	147.237.0.34	tikshuv.idf.il	Multiple Malformed HTTP Header Line from 45.79.103.178	Block	2
45.79.103.178	United States	147.237.0.34	tikshuv.idf.il	Multiple Malformed URL from 45.79.103.178	Block	2
139.162.13.205	Singapore	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
79.183.77.47	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/1740.png	Block	1
23.20.197.30	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
139.162.13.205	Singapore	147.237.76.42	refuah.idf.il	NULL Character in Header Name at	Block	1
89.185.1.39	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
139.162.13.205	Singapore	147.237.76.42	refuah.idf.il	Distributed Malformed URL	Block	1
80.246.133.140	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
24.114.84.201	Canada	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
139.162.13.205	Singapore	147.237.76.42	refuah.idf.il	NULL Character in Method [[#0]œ[[#0]][[#1]][[#26]]+<M[[#0]][[#1]][[#0]][[#0]][[#1]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#1]][[#0]][[#0]]	Block	1
109.253.210.106	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.66.180	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in 147.237.72.166/main/giyus/general.aspx	Block	1
139.162.13.205	Singapore	147.237.76.42	refuah.idf.il	Distributed Unknown HTTP Request Method	Block	1
84.109.192.207	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
37.46.37.100	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.69	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.69	Block	1
113.66.41.40	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18318-en/dover.aspx/trackback/	Block	1
79.178.240.247	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
139.162.13.205	Singapore	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Header Name	Block	1
207.46.13.47	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
124.73.6.250	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1694-11734-he/cogat.aspx/trackback/	Block	1
79.179.119.52	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
139.162.13.205	Singapore	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method [[#0]œ[[#0]][[#1]][[#26]]+<M[[#0]][[#1]][[#0]][[#0]][[#1]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#1]][[#0]][[#0]]	Block	1
87.12.200.87	Italy	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1

09-10-2016-01:06:42 to 09-10-2016-02:06:42