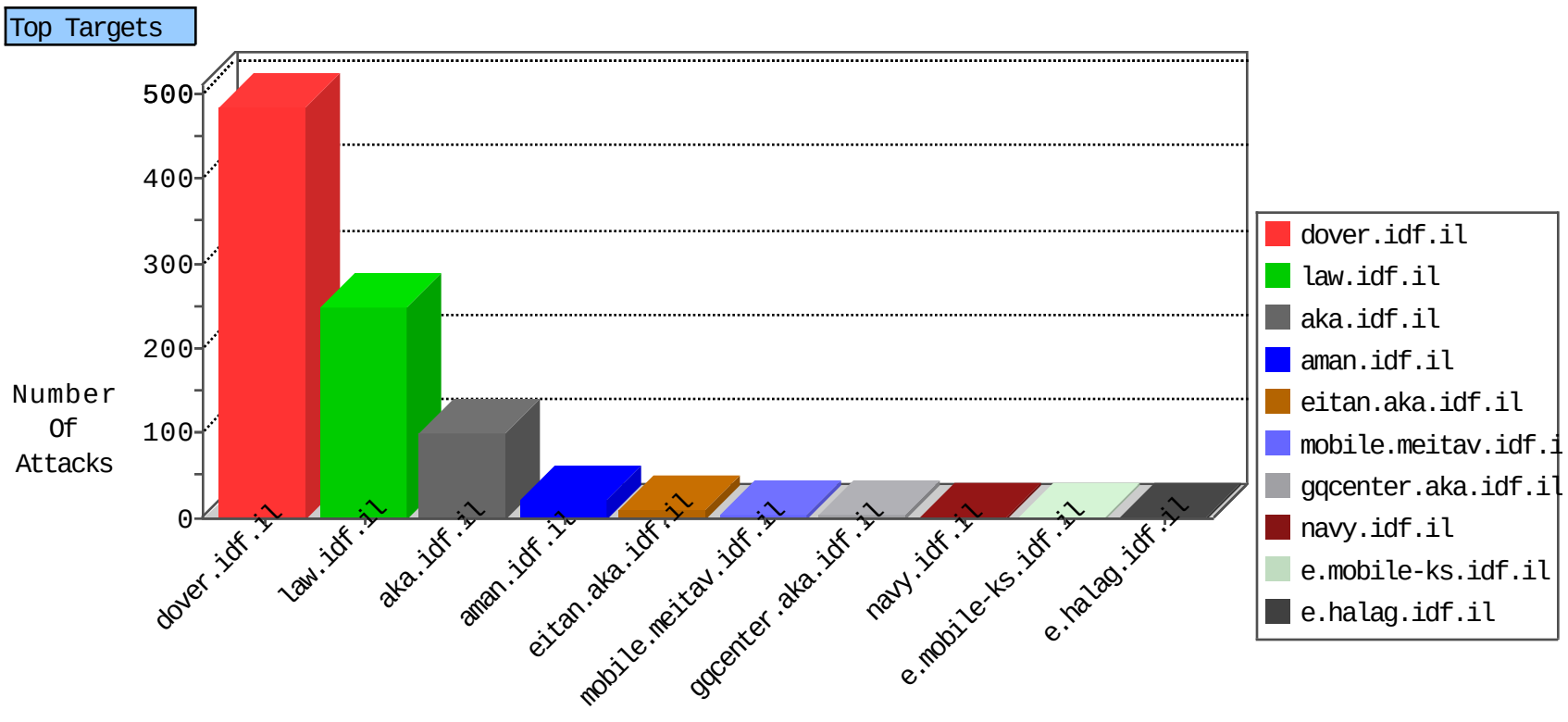
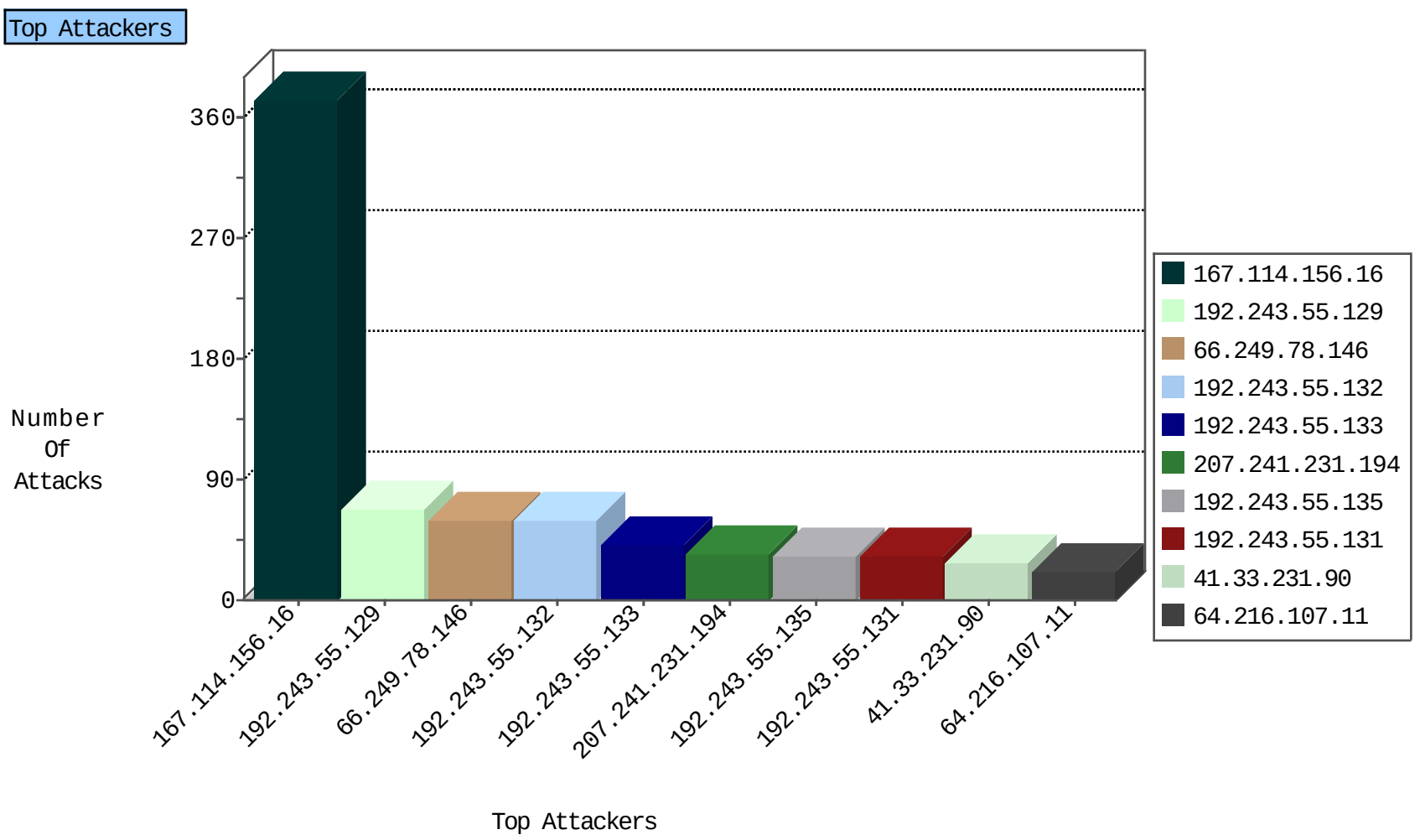
04-23-2016-05:04:06 to 04-23-2016-06:04:06

IDF Under Attack
Daily Report





04-23-2016-05:04:06 to 04-23-2016-06:04:06

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	HTTP-POST-Segmented-DoS	dest-reset	17264
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
94.102.49.116	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
185.103.252.98	Russian Federation	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
192.243.55.132	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
183.60.48.25	China	147.237.76.44	e.refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	1

04-23-2016-05:04:06 to 04-23-2016-06:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-23-2016-05:04:06 to 04-23-2016-06:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
185.130.5.99	147.237.77.61	Lithuania	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
76.181.249.213	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.99	147.237.76.34	Lithuania	yohalan.idf.il	ET SCAN Potential SSH Scan	1
58.218.211.11	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.0.35	Lithuania	akaws.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
40.84.148.3	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
219.148.198.41	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
162.244.15.191	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
219.148.198.41	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
110.143.44.114	147.237.8.46	Australia	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
187.160.213.25	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.248.171.19	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.99	147.237.77.176	Lithuania	matpash.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.99	147.237.76.202	Lithuania	e.halag.idf.il	ET SCAN Potential SSH Scan	1
58.218.211.11	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.8.27	Lithuania	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
58.218.211.11	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.0.34	Lithuania	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
40.114.42.13	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
40.84.148.3	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1
219.148.198.41	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
162.244.15.191	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
219.148.198.41	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
162.244.15.191	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
98.126.197.186	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.99	147.237.77.233	Lithuania	atal.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1

04-23-2016-05:04:06 to 04-23-2016-06:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
207.241.231.194	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	31
64.216.107.11	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
178.62.96.187	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.129	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
198.58.103.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.132	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
192.243.55.129	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
143.176.129.11	Netherlands	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
192.243.55.132	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.131	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.133	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.133	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
40.77.167.52	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.241.231.194	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.135	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.131	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
31.154.177.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	3
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
66.249.64.98	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
157.55.39.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

04-23-2016-05:04:06 to 04-23-2016-06:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
62.210.252.207	France	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
143.176.129.11	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en/	Block	1
174.129.228.67	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
5.255.253.34	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
68.180.230.184	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1

04-23-2016-05:04:06 to 04-23-2016-06:04:06