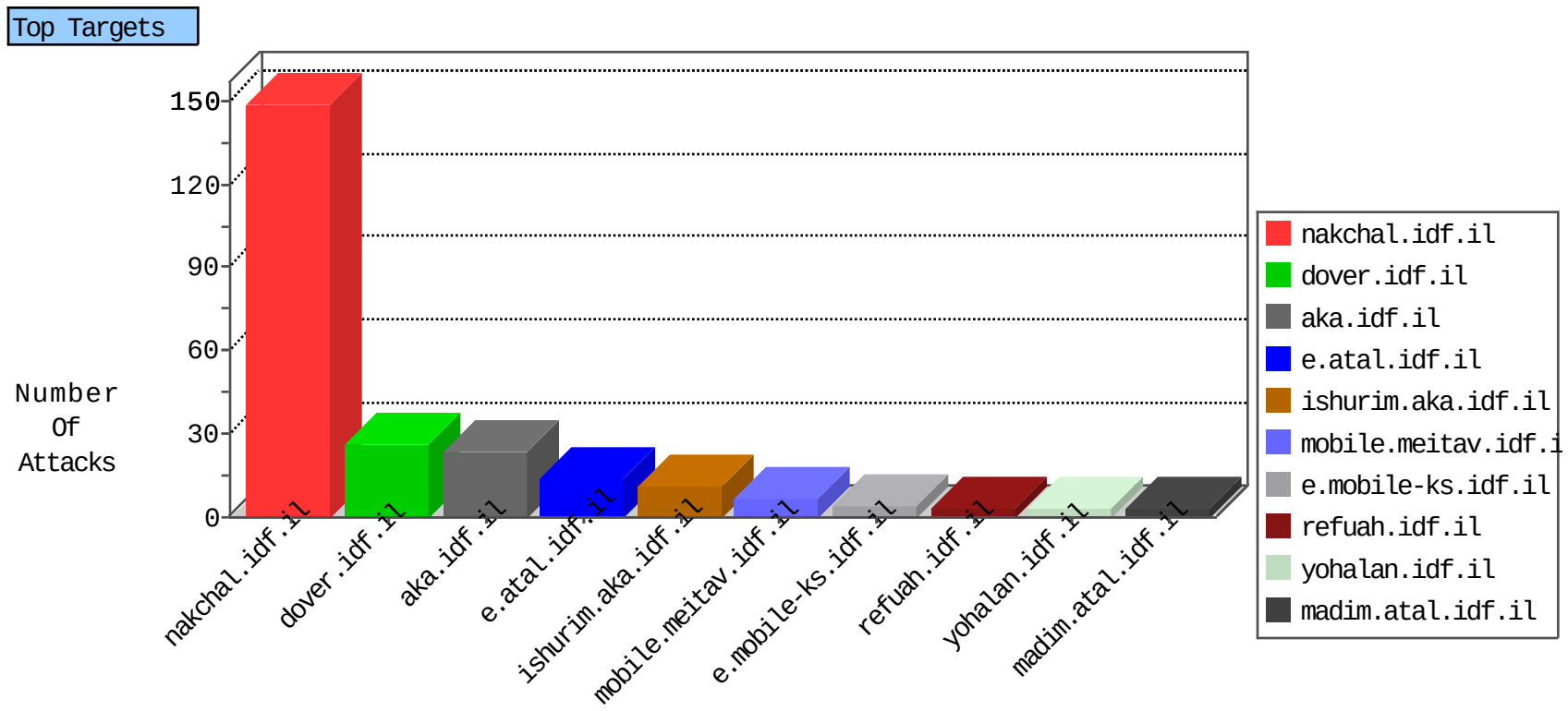
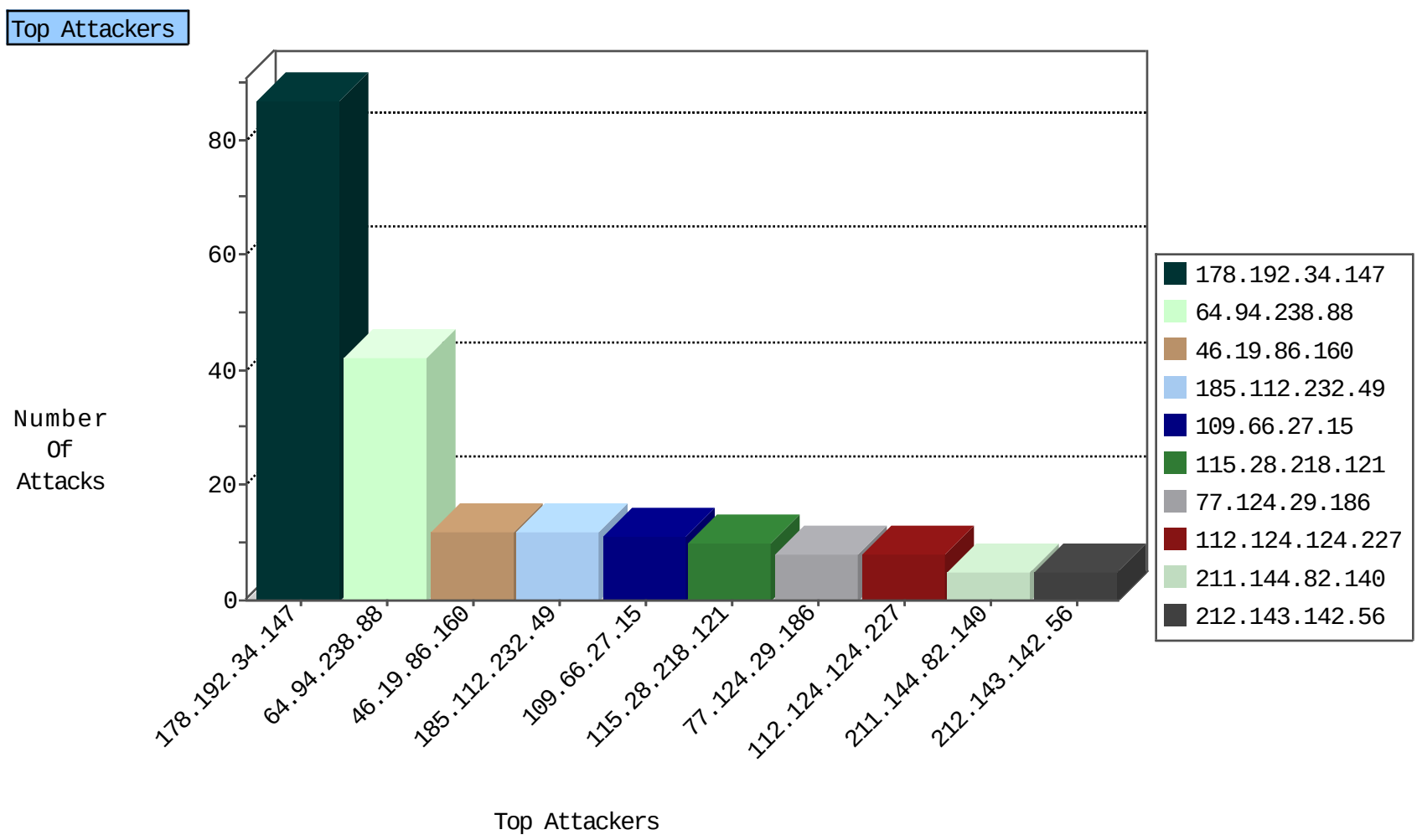
09-28-2016-04:04:04 to 09-28-2016-05:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-28-2016-04:04:04 to 09-28-2016-05:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
183.60.48.25	China	147.237.76.44	e.refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	1

09-28-2016-04:04:04 to 09-28-2016-05:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.251.184.38	France	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	2
151.80.31.155	France	147.237.77.234	halag.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

09-28-2016-04:04:04 to 09-28-2016-05:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
211.144.82.140	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
211.144.82.140	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
125.209.115.37	147.237.76.39	Pakistan	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.76.118	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
36.72.228.72	147.237.8.28	Indonesia	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1
36.72.228.72	147.237.8.28	Indonesia	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
211.144.82.140	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
211.144.82.140	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
211.144.82.140	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
113.240.250.154	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.141	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
36.72.228.72	147.237.8.28	Indonesia	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1

09-28-2016-04:04:04 to 09-28-2016-05:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	19
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	18
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	16
178.192.34.147	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
64.94.238.88	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	9
64.94.238.88	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	9
64.94.238.88	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
64.94.238.88	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
185.112.232.49	Iraq	147.237.76.201	e.atal.idf.il	drop	First packet isn't SYN	drop	8
77.124.29.186	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
46.19.86.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
64.94.238.88	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.86.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
124.82.45.169	Malaysia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.66.27.15	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.66.27.15	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
115.28.218.121	China	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
187.110.228.2	Brazil	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
109.66.27.15	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
112.124.124.227	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
115.28.218.121	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
125.209.115.37	Pakistan	147.237.76.39	mobile.meitav.idf.i	drop	First packet isn't SYN	drop	2
80.246.137.47	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
115.28.218.121	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
185.112.232.49	Iraq	147.237.76.201	e.atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	2
112.124.124.227	China	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
46.19.85.53	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
109.66.27.15	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
68.180.231.57	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
185.112.232.49	Iraq	147.237.76.201	e.atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
115.28.218.121	China	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
112.124.124.227	China	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
52.198.122.46	Japan	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
137.226.113.7	Germany	147.237.76.34	yohalan.idf.il	drop		drop	1
115.28.218.121	China	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
180.97.106.161	China	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.25	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.247.252	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
180.97.106.37	China	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
79.178.180.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.79	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
137.226.113.7	Germany	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.162	China	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.26	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
52.198.122.46	Japan	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
112.124.124.227	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
180.97.106.37	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
172.56.26.146	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-28-2016-04:04:04 to 09-28-2016-05:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.110.233.19	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	4
77.138.115.145	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	2
217.132.190.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.76.118	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
157.55.39.28	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
70.31.203.22	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
157.55.39.60	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
66.249.66.197	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-22257-he/idfgdover.aspx	Block	1
66.249.76.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
98.192.185.99	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1

09-28-2016-04:04:04 to 09-28-2016-05:04:04