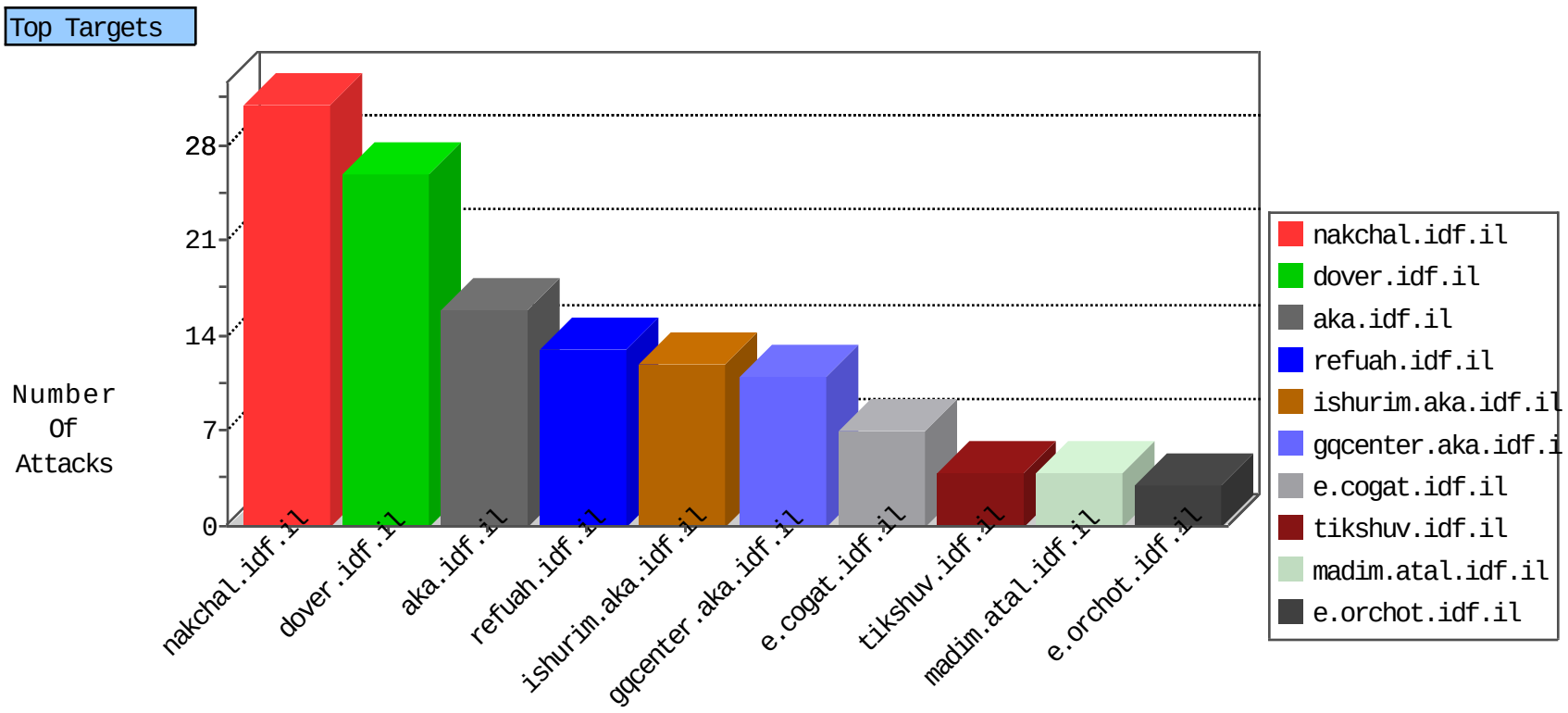
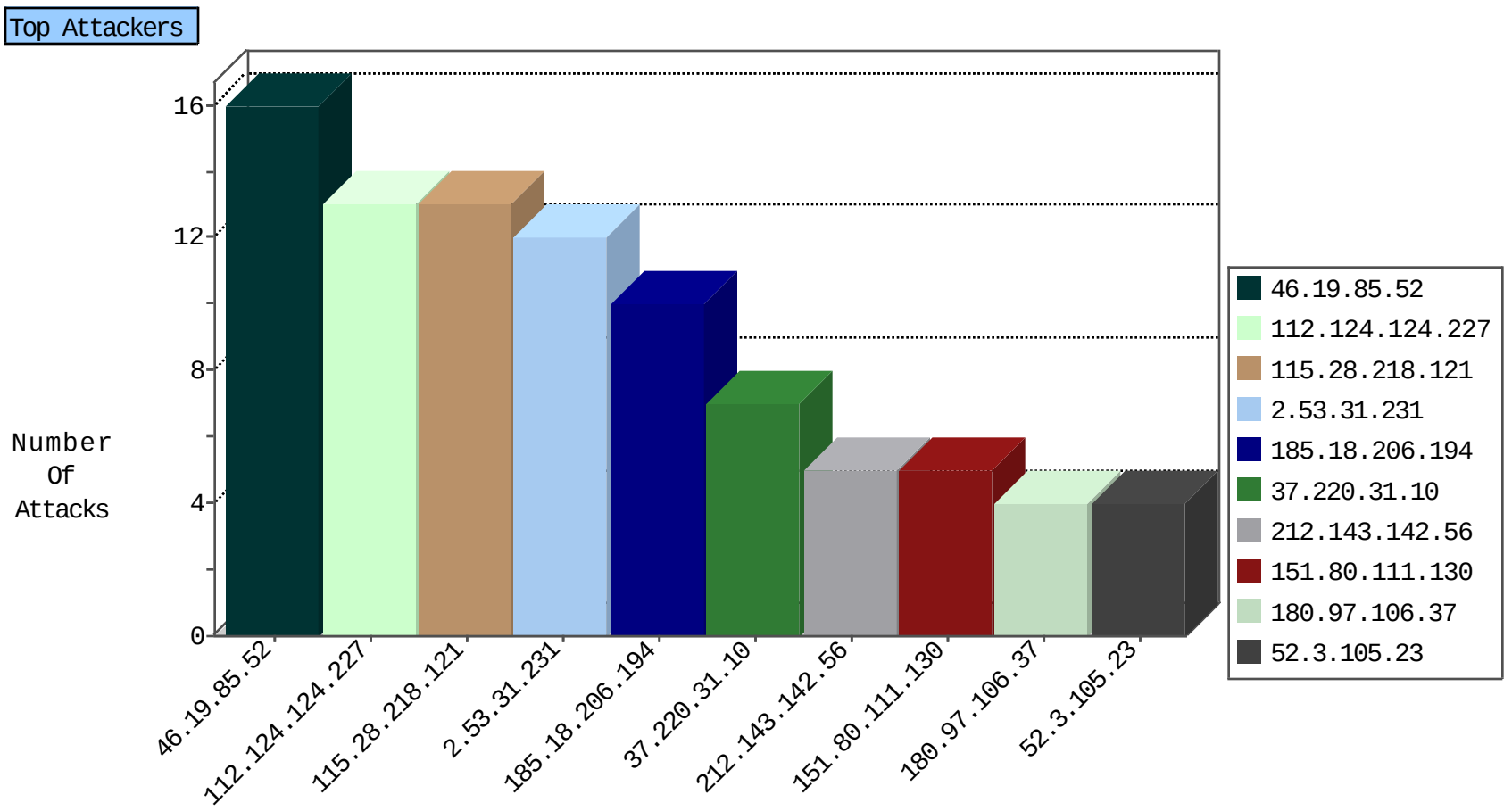
09-28-2016-03:04:06 to 09-28-2016-04:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-28-2016-03:04:06 to 09-28-2016-04:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.174.94.235	Netherlands	147.237.76.177	ncore.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1

09-28-2016-03:04:06 to 09-28-2016-04:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-28-2016-03:04:06 to 09-28-2016-04:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.220.31.10	147.237.77.61	United Kingdom	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	2
113.240.250.154	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.154	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
62.150.255.205	147.237.72.217	Kuwait	e.idf.il	ET SCAN NMAP -sS window 3072	1
221.229.172.116	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
62.150.255.205	147.237.72.217	Kuwait	e.idf.il	ET SCAN NMAP -f -sS	1
221.229.172.116	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
187.162.200.249	147.237.77.205	Mexico	prisha.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
41.39.177.14	147.237.77.226	Egypt	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
163.172.129.15	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
41.39.177.14	147.237.77.226	Egypt	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
117.158.160.211	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
116.77.72.71	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
113.240.250.154	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.154	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
221.229.172.116	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
62.150.255.205	147.237.72.217	Kuwait	e.idf.il	ET SCAN NMAP -sS window 2048	1
221.229.172.116	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
209.95.50.84	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.161.40.17	147.237.76.147	Russian Federation	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.141.198	147.237.8.28	Switzerland	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
41.39.177.14	147.237.77.226	Egypt	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
117.158.160.211	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
37.220.31.10	147.237.77.61	United Kingdom	e.cogat.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
116.77.72.71	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1

09-28-2016-03:04:06 to 09-28-2016-04:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
2.53.31.231	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.18.206.194	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
176.13.17.28	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
115.28.218.121	China	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
185.18.206.194	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
37.220.31.10	United Kingdom	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
112.124.124.227	China	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
185.18.206.194	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
115.28.218.121	China	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
112.124.124.227	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
157.55.2.158	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
115.28.218.121	China	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
80.246.136.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
52.3.105.23	United States	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	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
95.221.204.170	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
37.220.31.10	United Kingdom	147.237.77.61	e.cogat.idf.il	drop	First packet isn't SYN	drop	2
112.124.124.227	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
115.28.218.121	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
141.212.122.64	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
78.109.28.237	Ukraine	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
52.3.105.23	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
141.212.122.79	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
5.22.134.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.66.24.133	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.161	China	147.237.0.33	idf.il	drop		drop	1
68.64.167.142	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
151.80.111.130	France	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
41.77.138.90	Egypt	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
141.212.122.72	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
80.246.136.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
180.97.106.37	China	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
52.3.105.23	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
151.80.111.130	France	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.46.41.205	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.94	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
180.97.106.161	China	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
69.60.111.84	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
45.58.118.202	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
141.212.122.73	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
180.97.106.37	China	147.237.0.35	akaws.idf.il	drop		drop	1
151.80.111.130	France	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
37.46.41.205	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
137.116.71.170	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
180.97.106.162	China	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

09-28-2016-03:04:06 to 09-28-2016-04:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.113	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	1
66.249.69.127	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8860-he/refuah.aspx	Block	1
185.27.106.131	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
61.8.202.103	Singapore	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/tizmoret/gallery/showpicture.asp	Block	1
185.27.106.131	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
46.19.85.129	Israel	147.237.72.166	aka.idf.il	Unknown Parameter asm in www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	None	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/tizmoret/gallery/	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
157.55.39.104	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1

09-28-2016-03:04:06 to 09-28-2016-04:04:06