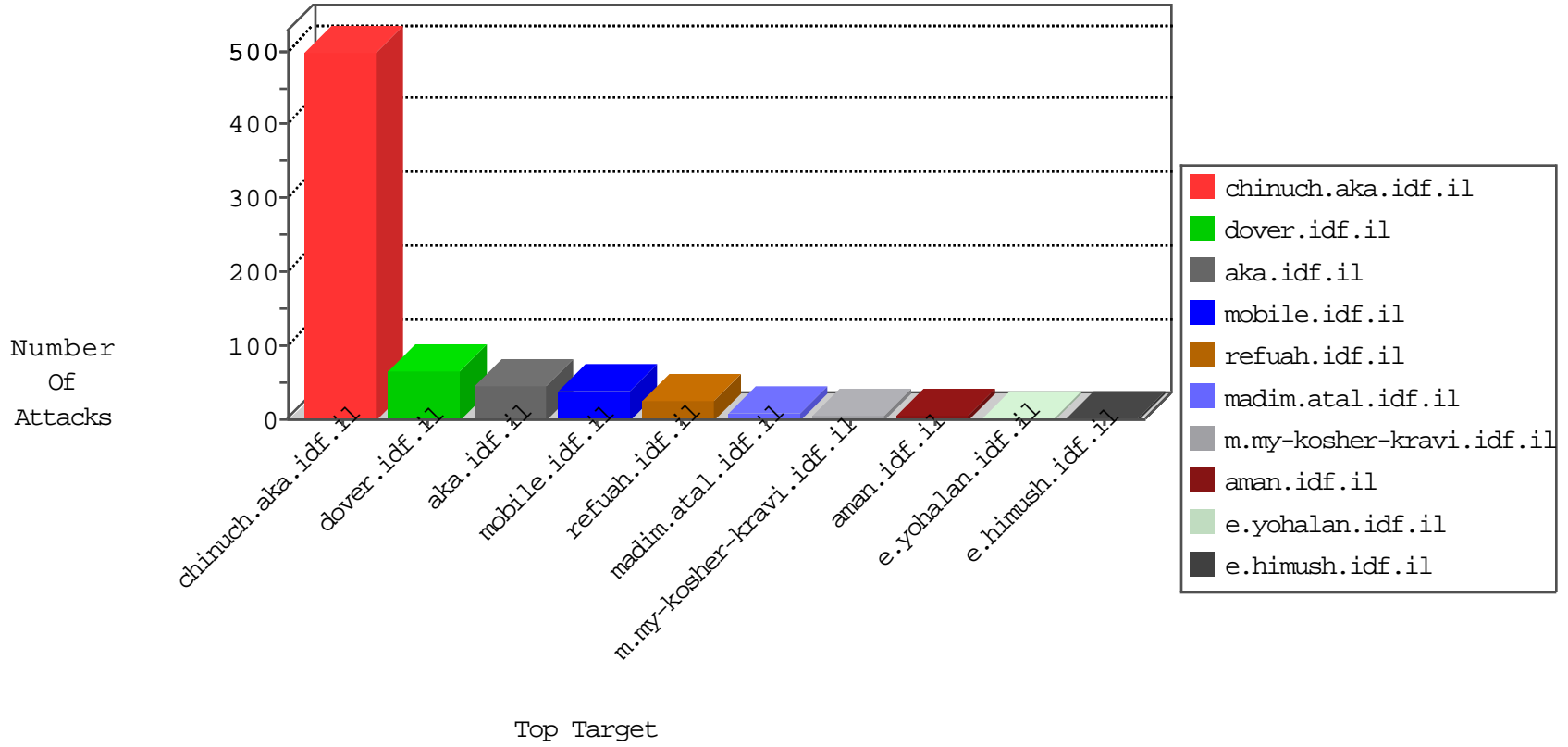


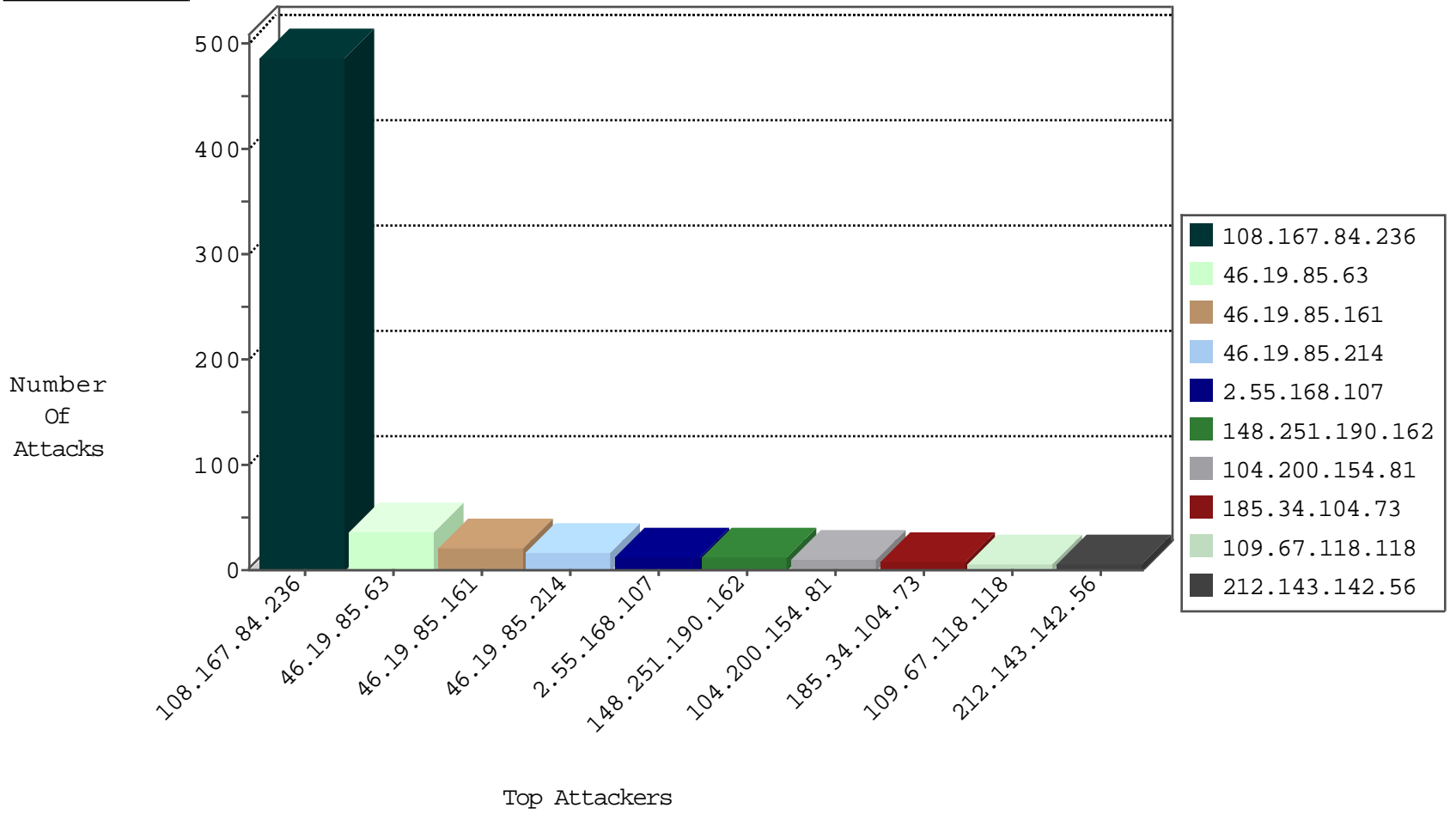
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
45.32.204.130	Netherlands	147.237.76.202	e.halag.idf.il	Black List	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
148.251.190.162	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	8
148.251.190.162	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
148.251.190.162	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
71.6.146.185	United States	147.237.0.17	m.my-kosher-kravi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.201.236.50	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
66.249.64.145	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	1
46.172.91.21	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
185.129.148.230	147.237.77.74	Latvia	law.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.144.18	147.237.0.17	Switzerland	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
163.172.238.45	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN NMAP -sS window 1024	1
120.63.143.13	147.237.76.30	India	himush.idf.il	ET SCAN NMAP -sS window 4096	1
109.60.153.178	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
91.201.236.50	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.50	147.237.76.198	Ukraine	e.yohalan.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
54.144.119.103	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
46.161.40.17	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.144.18	147.237.76.42	Switzerland	refuah.idf.il	ET SCAN Potential SSH Scan	1
163.172.238.45	147.237.76.148	United Kingdom	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.76.38	United Kingdom	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
115.148.99.2	147.237.76.177	China	ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
95.163.144.203	147.237.76.176	Russian Federation	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
108.167.84.236	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	488
46.19.85.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.85.214	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	17
2.55.168.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.63	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.63	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
104.200.154.81	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	10
46.19.85.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.102.195.21	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
84.229.42.101	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.118.118	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
75.110.105.152	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
185.3.147.230	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.67.118.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
76.175.32.222	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
80.246.138.40	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.135	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.219	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
64.246.187.42	United States	147.237.72.166	aka.idf.il	Header Rejection	header rejection pattern found in request	monitor	2
187.153.214.213	Mexico	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
144.139.140.64	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
207.46.13.21	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
76.175.32.222	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
176.13.10.242	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
185.34.104.73	Ireland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.102.242.28	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.253.159.184	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.108	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
185.34.104.73	Ireland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1
176.13.242.235	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.67.37.186	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.61	United States	147.237.0.33	idf.il	drop		drop	1
208.109.181.132	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.34.104.73	Ireland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
24.159.6.34	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.173	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
185.34.104.73	Ireland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
184.105.247.207	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.22.134.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.34.104.73	Ireland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
24.159.6.34	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
141.212.122.174	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
85.130.170.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.22.134.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.76	United States	147.237.76.34	yochalan.idf.il	drop		drop	1
46.19.86.78	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
185.34.104.73	Ireland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.232.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.128.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.46.37.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
157.55.39.21	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/haredim/maslulimlist.aspx	None	1
207.46.13.21	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/smalim/html/1.asp	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9032-he/refuah.aspx	Block	1
207.46.13.56	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/sachar/faq.aspx	None	1
157.55.39.21	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
40.77.169.100	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-14686-he/dover.aspx (hebrew)	Block	1
207.46.13.22	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/captcha.ashx	Block	1
79.176.59.226	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct161 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
157.55.39.54	United States	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1
66.102.6.4	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/sachar	Block	1
207.46.13.35	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/captcha.ashx	Block	1
84.109.10.19	Israel	147.237.72.166	aka.idf.il	Unknown Parameter asm in www.aka.idf.il/main/gyus/yahash2017/lobby.aspx	None	1
157.55.39.60	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/general.aspx	Block	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/gyus/booklets.aspx	Block	1
207.46.13.56	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/drushim/info.aspx	None	1
157.55.39.251	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation asperrorpath in www.idf.il/error.htm	Block	1
207.46.13.56	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/haredim/gallery.aspx	None	1