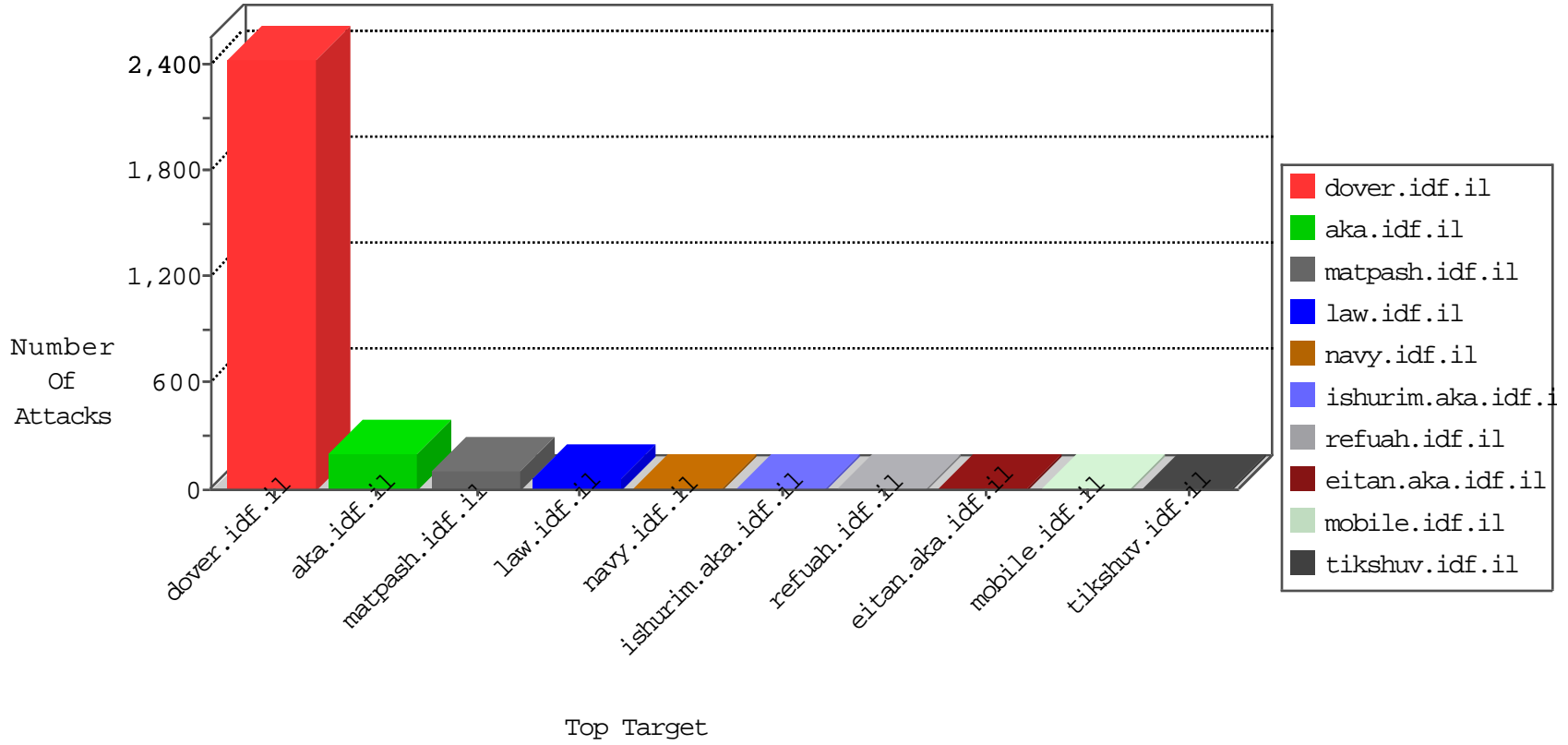


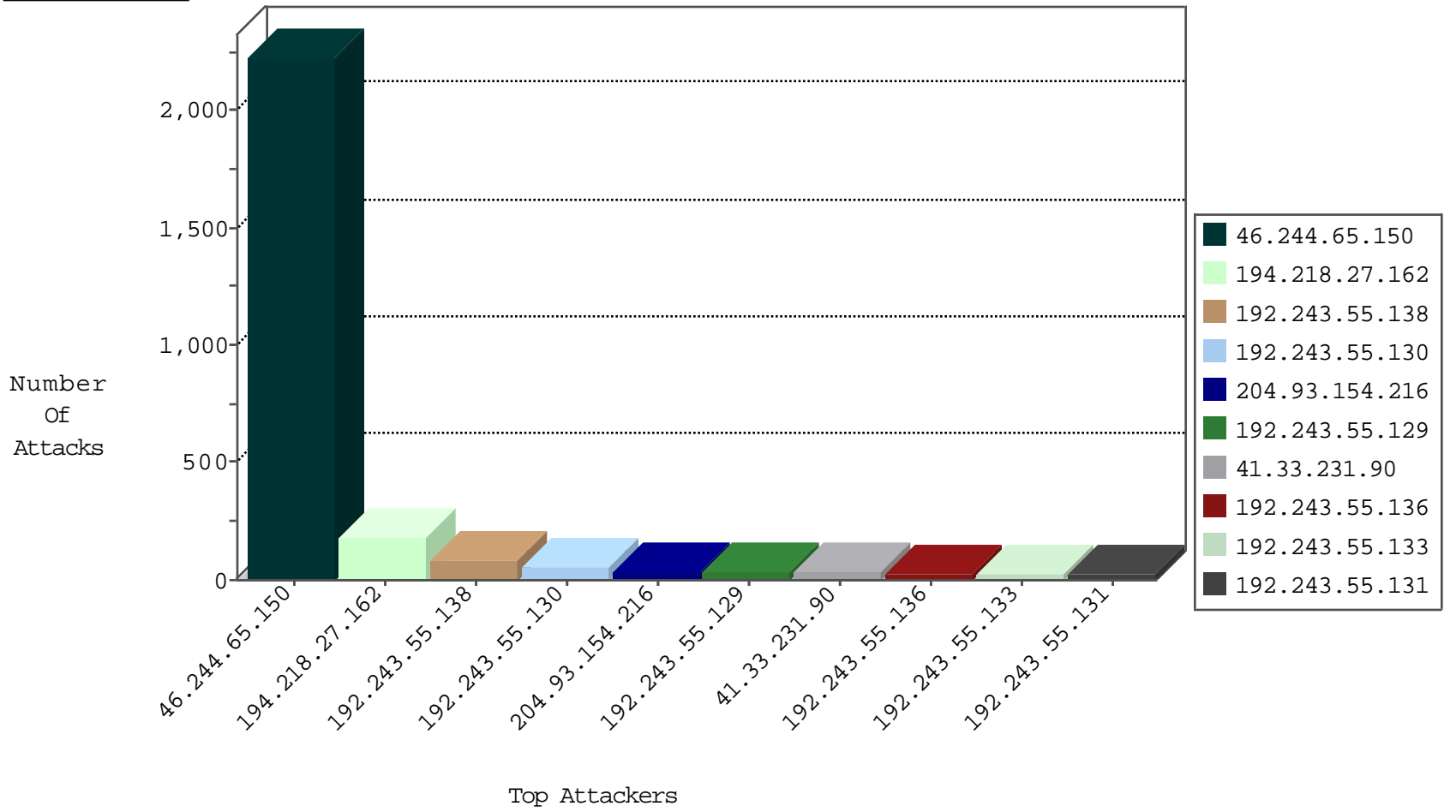
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.244.65.150	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	2222
204.93.154.216	United States	147.237.77.216	dover.idf.i	TCP Scan (vertical)	drop	154
208.117.68.180	United States	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	8
168.235.197.242	United States	147.237.77.216	dover.idf.i	JLM_Purple_Con_Limit_Http	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	1
168.235.197.242	United States	147.237.77.216	dover.idf.i	JLM_Under_Attack_Con_Http	drop	1
46.246.123.44	Sweden	147.237.0.33	idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
61.135.189.119	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
149.202.48.176	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
149.202.48.176	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
173.208.136.170	United States	147.237.77.176	matpash.idf.il	C1000016: HTTP: administrator in URI	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
87.70.18.67	Israel	147.237.76.86	navy.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
175.99.87.209	147.237.76.42	Taiwan	refuah.idf.il	ET SCAN NMAP -f -sS	1
104.232.98.38	147.237.77.234		halag.idf.il	ET SCAN NMAP -sS window 3072	1
104.171.122.167	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
93.113.125.11	147.237.72.217	Romania	e.idf.il	ET SCAN NMAP -sS window 1024	1
52.90.244.8	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
40.117.92.242	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 4096	1
209.126.116.147	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
175.99.87.209	147.237.76.42	Taiwan	refuah.idf.il	ET SCAN NMAP -sS window 2048	1
106.38.241.106	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
104.232.98.38	147.237.77.234		halag.idf.il	ET SCAN NMAP -sS window 1024	1
104.171.122.167	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	147.237.0.15	Turkey	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
40.117.92.242	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
220.231.195.122	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 3072	1
175.99.87.209	147.237.76.42	Taiwan	refuah.idf.il	ET SCAN NMAP -sS window 4096	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	120
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	60
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
192.243.55.138	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.138	Dominica	147.237.77.176	matpash.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	7
192.243.55.136	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.138	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.138	Dominica	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.138	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.138	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence		monitor	4
192.243.55.130	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.138	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.130	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.130	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.244.65.150	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
192.243.55.129	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
93.113.125.11	Romania	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.253.156.47	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.149.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.123.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
192.243.55.130	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence		monitor	2
192.243.55.138	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.113.125.11	Romania	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to /	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/drushi	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.66.72	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.66.72	Block	1
213.57.42.160	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakchal.idf.il/1073-he/nakhal.aspx	Block	1
37.203.214.2	Sweden	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
107.150.42.36	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.yun.ph/	Block	1
66.249.66.75	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/gyus/forum/asp/showforum.asp	Block	1
213.57.42.160	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 213.57.42.160	Block	1
77.237.138.202	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
37.203.214.2	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
184.105.139.68	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
66.249.66.78	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/yohalan/main/main.asp	Block	1
82.199.97.68	Russian Federation	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/info.asp	Block	1
46.244.65.150	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.243.55.137	Dominica	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	1