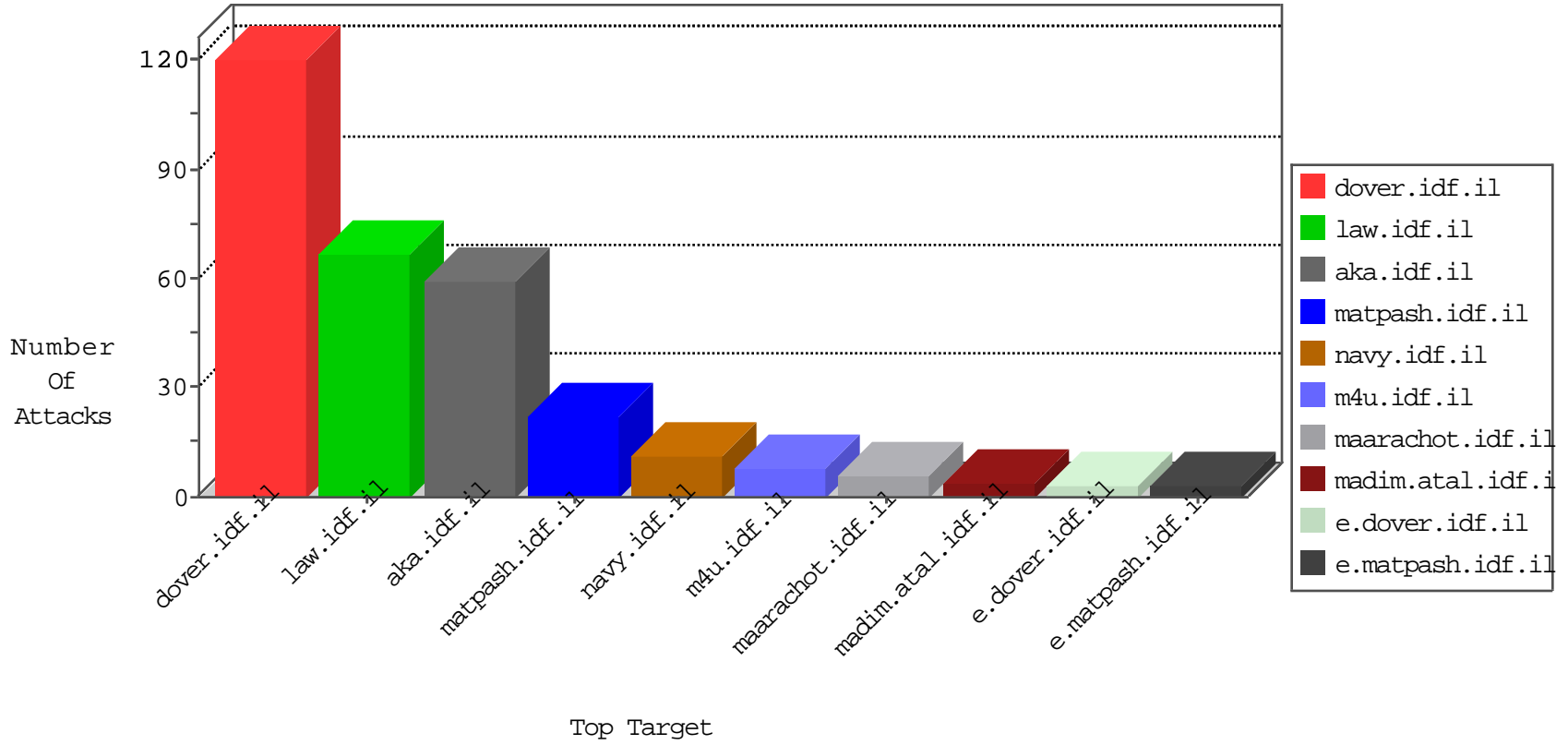


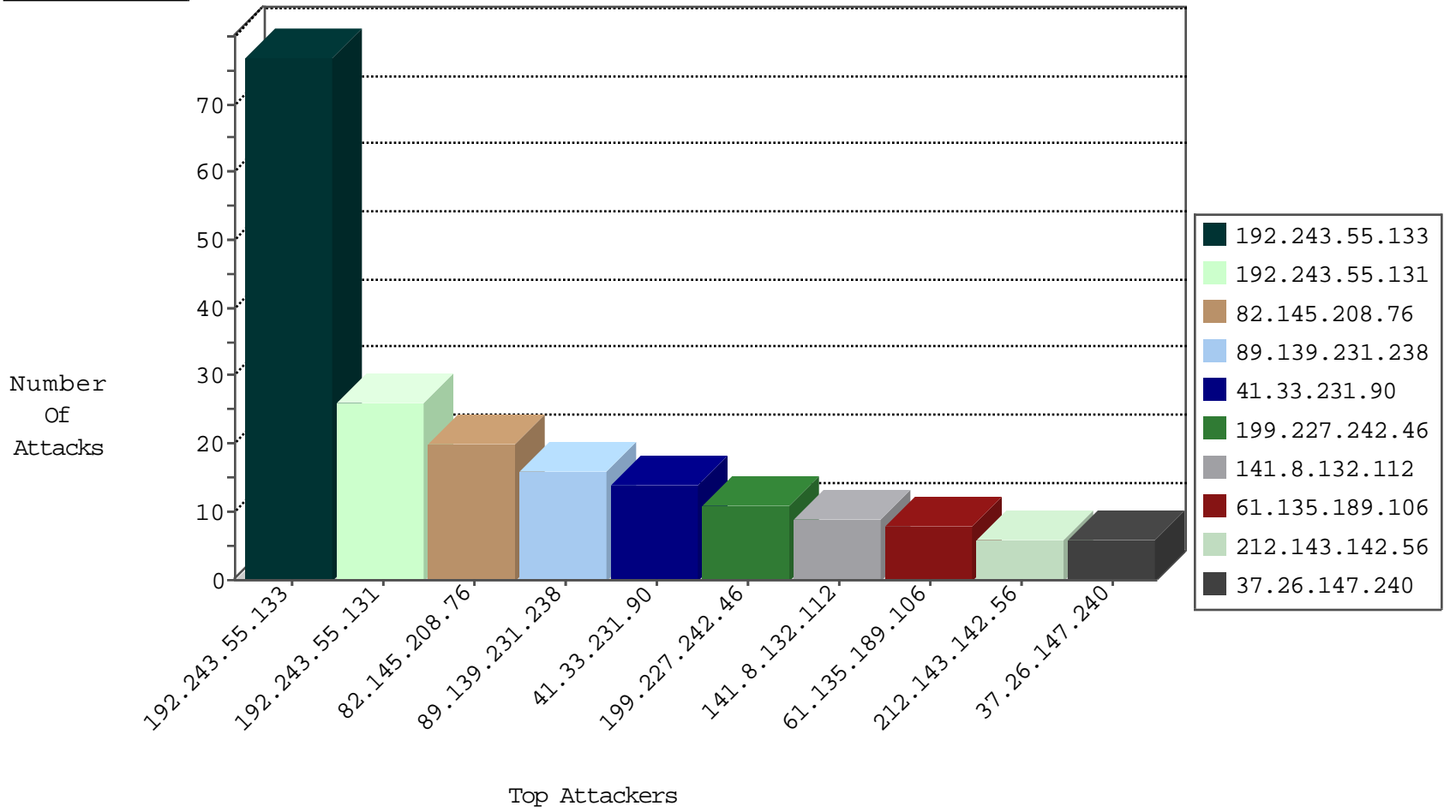
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.208.76	Europe	147.237.77.176	matpash.idf.il	Block_Tp_Web_In	drop	20
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	2
179.43.144.33	Switzerland	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.2	United States	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
162.216.114.158	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.135.189.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
91.121.169.194	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
199.30.25.99	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.233	atal.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
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
157.55.39.179	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

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	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
185.56.82.54	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
128.127.0.45	147.237.76.177	Italy	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.64	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.77.212	Latvia	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
185.56.82.54	147.237.0.33	Netherlands	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
128.127.0.45	147.237.76.177	Italy	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
128.127.0.45	147.237.76.177	Italy	ncore.idf.il	ET SCAN NMAP -f -sS	1
213.136.91.26	147.237.0.16	Germany	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.77.178	Latvia	e.matpash.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
185.72.179.221	147.237.77.176		matpash.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
89.139.231.238	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
199.227.242.46	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.133	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.133	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
192.243.55.133	Dominica	147.237.77.74	law.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	6
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.22.130.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
189.218.162.104	Mexico	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
91.200.12.141	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	4
201.173.134.198	Mexico	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
31.210.188.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.131	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
61.135.189.106	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
77.127.14.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.146.44.155	Italy	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.123.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.253.212.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.195.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.52.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.108.5.233	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
91.200.12.7	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	2
195.60.232.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
192.243.55.131	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
37.26.147.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		alert	2
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
37.26.147.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
37.26.147.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
188.32.55.220	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.113	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.126.113.80	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.198	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.54.83.209	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.187.253.17	Iran, Islamic Republic of	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.75	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.238.120.22	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	4
208.115.113.88	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/giyus/forum/asp/showforum.asp	Block	4
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
68.132.177.198	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtEmail in www.idf.il/1038-en/dover.aspx	Block	2
185.32.179.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/dover.aspx.	Block	1
31.210.188.115	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct109 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.64.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
112.198.103.96	Philippines	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.93.52	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
157.55.39.252	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/rabanut/62048	Block	1
65.55.210.232	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/yoman/yoman.asp	Block	1
178.212.100.47	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar'a=0	Block	1
220.255.146.81	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
88.75.189.79	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
24.199.9.162	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1