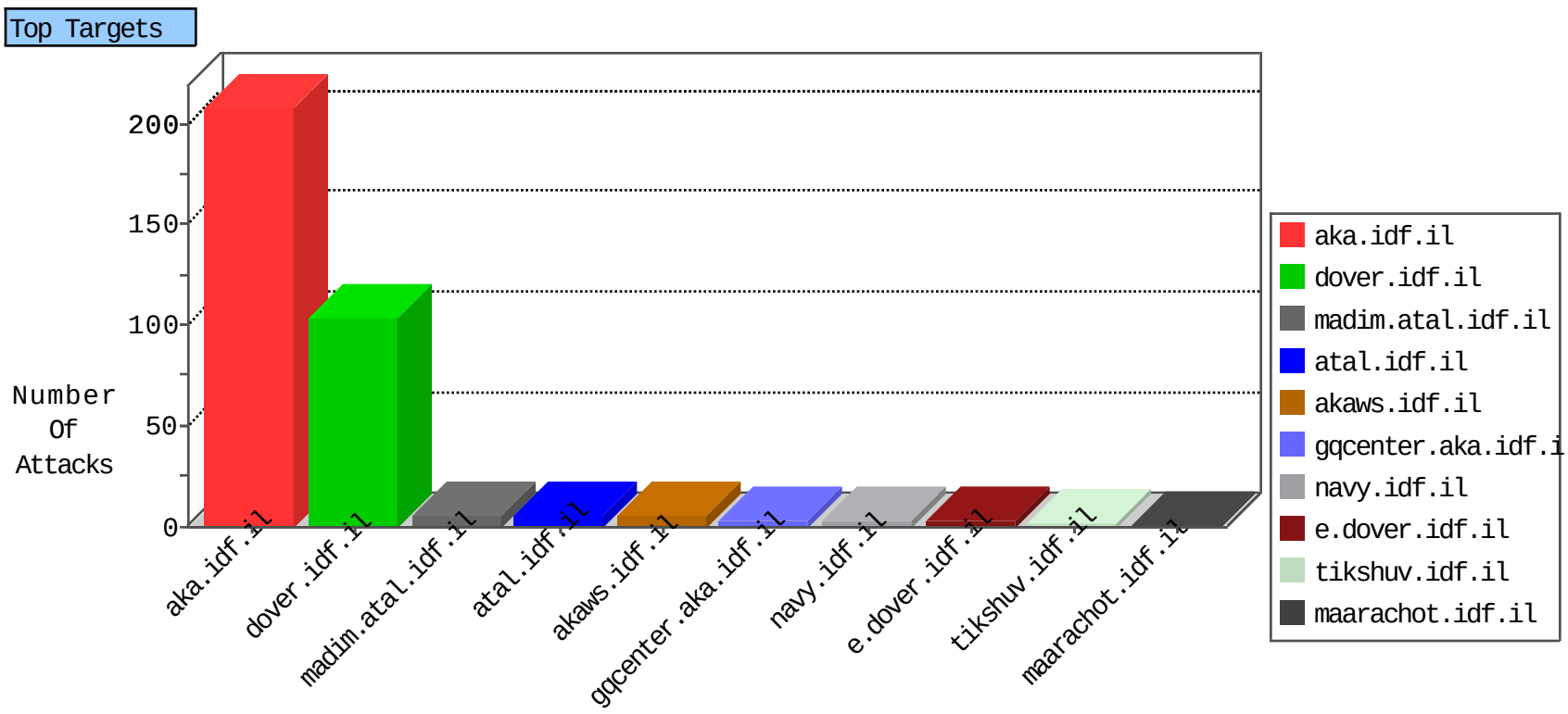
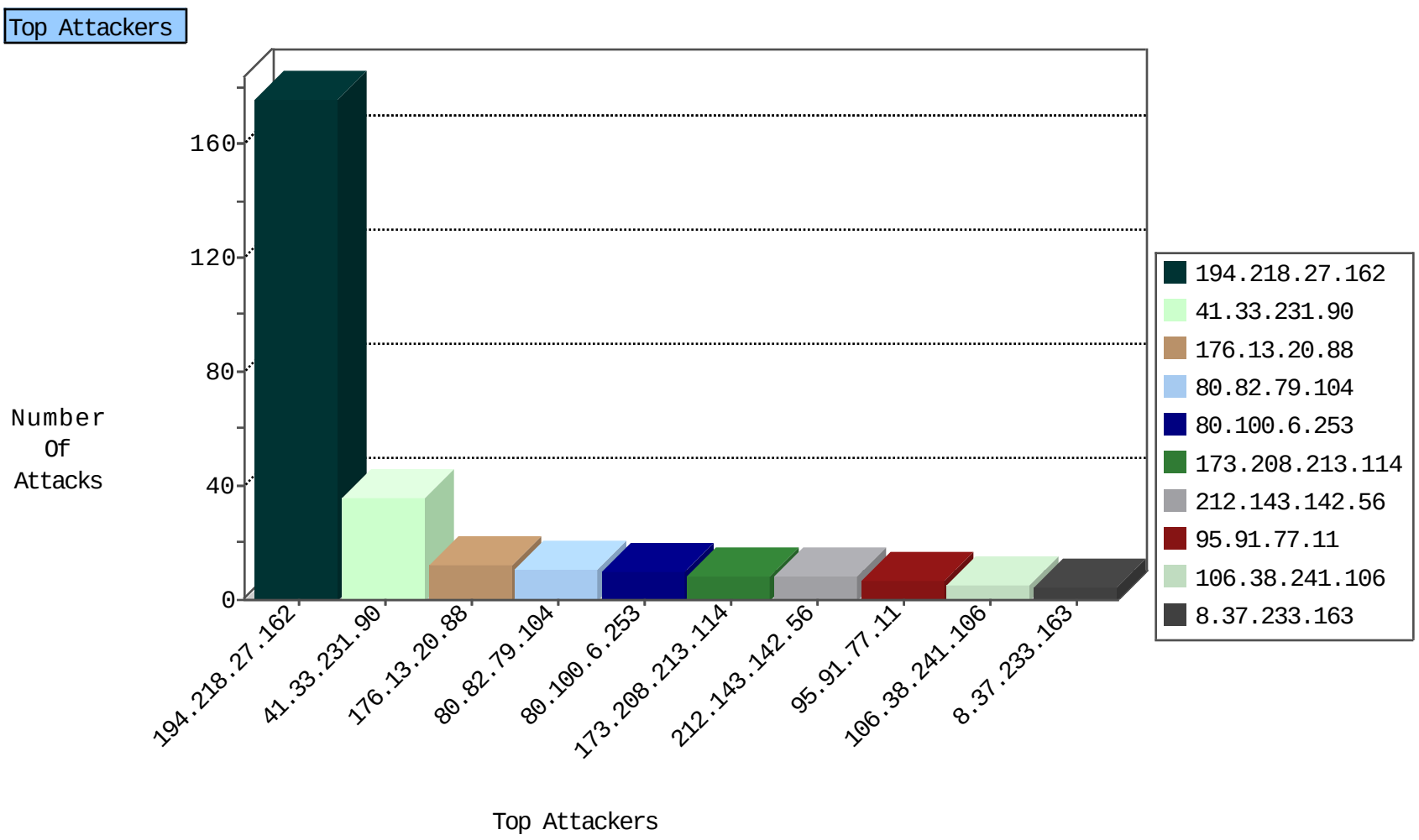
03-01-2016-03:04:00 to 03-01-2016-04:04:00

IDF Under Attack Daily Report





03-01-2016-03:04:00 to 03-01-2016-04:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.103.252.5		147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
91.121.183.16	France	147.237.0.35	akaws.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.130	United States	147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.77.212	e.dover.idf.il	Block_Udp_All_Nets	drop	1
61.160.194.228	China	147.237.0.35	akaws.idf.il	JLM_Purple_Con_Limit_Http	drop	1
89.248.172.207	Netherlands	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.246		147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1

03-01-2016-03:04:00 to 03-01-2016-04:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.91.77.11	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
61.135.189.110	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
174.34.135.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
176.9.131.69	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
95.91.77.11	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
162.250.190.142	Canada	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1

03-01-2016-03:04:00 to 03-01-2016-04:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
188.191.21.221	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
125.252.13.129	147.237.76.30	Korea, Republic of	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.193	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
50.77.145.78	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
212.227.89.173	147.237.77.74	Germany	law.idf.il	ET SCAN Potential SSH Scan	1
188.191.21.221	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
159.122.223.130	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.38	147.237.77.170		maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
80.82.79.104	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1

03-01-2016-03:04:00 to 03-01-2016-04:04:00

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	116
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	58
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
176.13.20.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.100.6.253	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
173.208.213.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.178.107.230	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
109.67.167.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.103.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.171.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.181.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.111.39.33	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
85.214.155.116	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.29.78.38	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
45.32.233.86		147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.153	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
95.91.77.11	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
80.82.79.104	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.82.79.104	Netherlands	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.60.87.65	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.154	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
80.82.79.104	Netherlands	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.106.92.164		147.237.0.35	akaws.idf.il	drop		drop	1
80.82.79.104	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.154	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
80.82.79.104	Netherlands	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.82.79.104	Netherlands	147.237.0.33	idf.il	drop		drop	1
185.106.92.164		147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
113.76.90.199	China	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
80.82.79.104	Netherlands	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
159.226.95.66	China	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.38.241.106	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
80.89.7.218	Russian Federation	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
80.82.79.104	Netherlands	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
192.0.99.131	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.153	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
80.82.79.104	Netherlands	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.38.241.106	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
80.82.79.104	Netherlands	147.237.0.35	akaws.idf.il	drop		drop	1

03-01-2016-03:04:00 to 03-01-2016-04:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
8.37.233.163	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
131.253.25.251	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.69.26	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.69.26	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-15944-en/dover	Block	1
157.55.39.40	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
65.55.210.113	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
213.57.134.162	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1

03-01-2016-03:04:00 to 03-01-2016-04:04:00