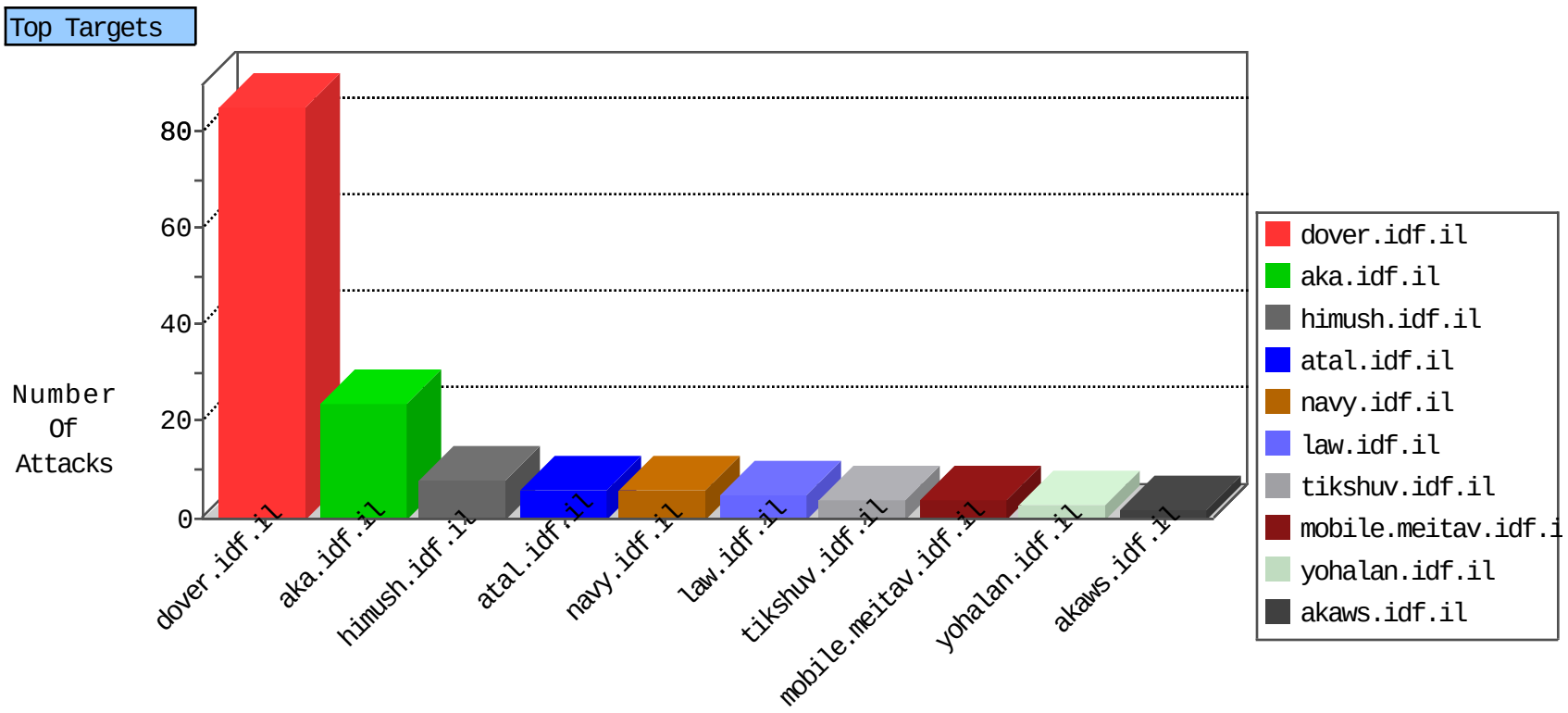
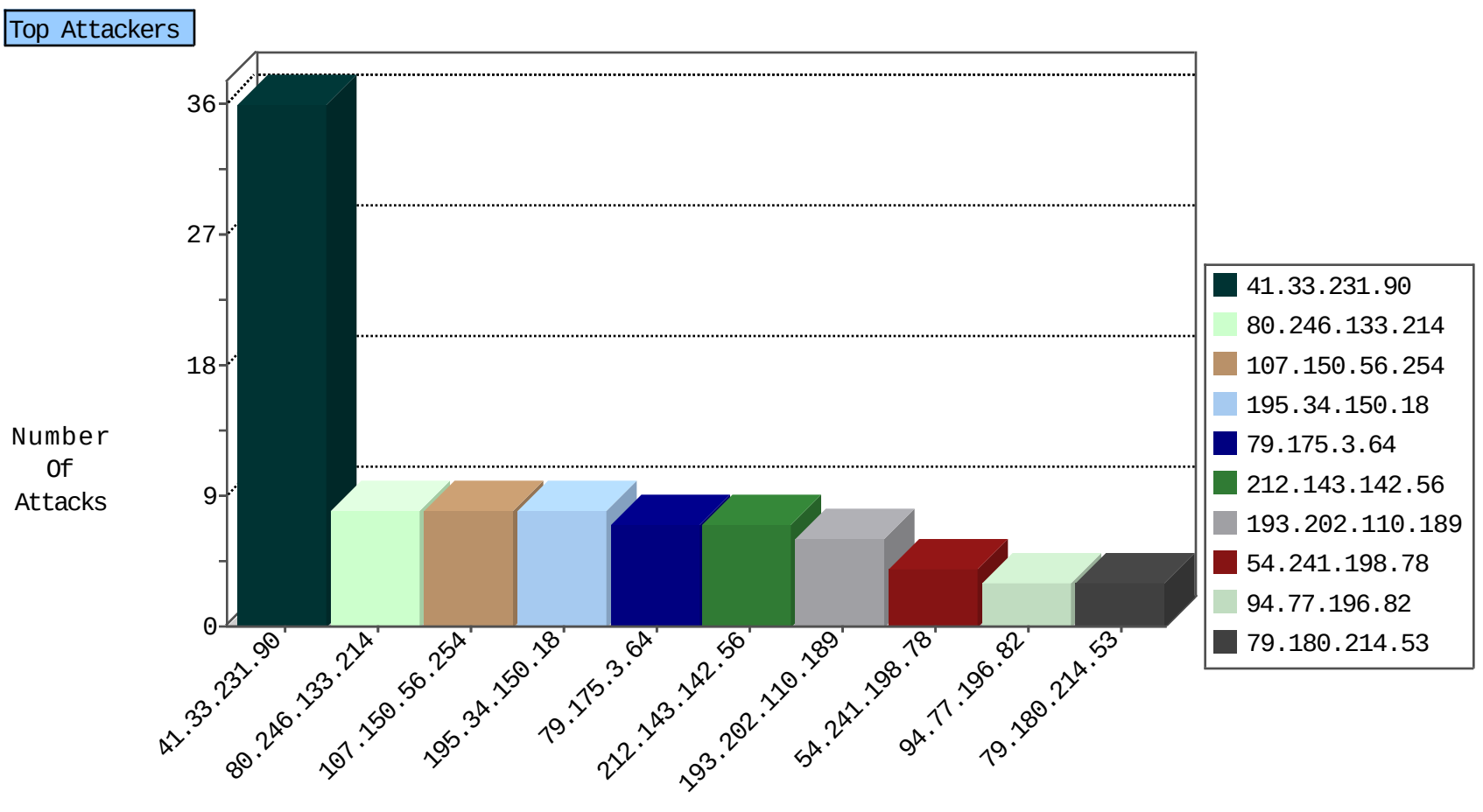
02-26-2016-03:04:04 to 02-26-2016-04:04:04

IDF Under Attack Daily Report





02-26-2016-03:04:04 to 02-26-2016-04:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.135.154.20	Czech Republic	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
31.206.69.70	Turkey	147.237.72.166	aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
204.42.253.2	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2
81.215.199.30	Turkey	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
208.100.26.228	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
198.23.190.39	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
208.100.26.228	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

02-26-2016-03:04:04 to 02-26-2016-04:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
107.150.56.254	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
69.30.215.130	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
107.150.56.254	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
107.150.56.254	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
2.54.52.135	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
61.135.189.103	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
151.80.31.151	Italy	147.237.72.166	aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	2
51.255.65.61	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.77	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.15	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
65.55.210.158	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
51.255.65.32	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

02-26-2016-03:04:04 to 02-26-2016-04:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.133.214	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
218.246.0.97	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.77.178	Sweden	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
108.61.228.113	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
64.53.35.15	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
208.109.252.167	147.237.76.86	United States	navy.idf.il	LOCAL_RULES - Request with the string install.php in it	1
193.105.134.220	147.237.77.234	Sweden	halag.idf.il	ET SCAN NMAP -sS window 1024	1
108.61.228.113	147.237.76.148	United States	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1

02-26-2016-03:04:04 to 02-26-2016-04:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
79.175.3.64	Russian Federation	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
193.202.110.189	Netherlands	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
54.241.198.78	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
82.81.26.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.180.214.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.187.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
50.18.94.121	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
148.251.13.51	Germany	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
192.0.113.82	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
106.38.241.106	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
66.240.192.138	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.201	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.68	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.206	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.195	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.59	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.202	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.148	United States	147.237.0.35	akaws.idf.il	drop		drop	1
87.67.241.14	Belgium	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.196	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
195.62.53.168	Russian Federation	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.22.129.234	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.205	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.149	United States	147.237.0.35	akaws.idf.il	drop		drop	1
184.105.247.215	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.196	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
136.243.16.208	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
208.109.252.167	United States	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.205	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.157	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
61.135.189.103	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.197	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.67	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
80.246.133.214	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.206	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.158	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

02-26-2016-03:04:04 to 02-26-2016-04:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
116.66.197.233	Nepal	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 116.66.197.233 (Open Mode)	None	1
207.46.13.21	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/sip_storage/files/5/2475.jpg	Block	1
134.249.54.139	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	1
208.109.252.167	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/install/index.php.bak	Block	1
54.85.55.6	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.107	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
60.209.5.30	China	147.237.77.74	law.idf.il	Malformed URL http-req	Block	1
178.216.202.190	Poland	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	Block	1
193.252.118.176	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1

02-26-2016-03:04:04 to 02-26-2016-04:04:04