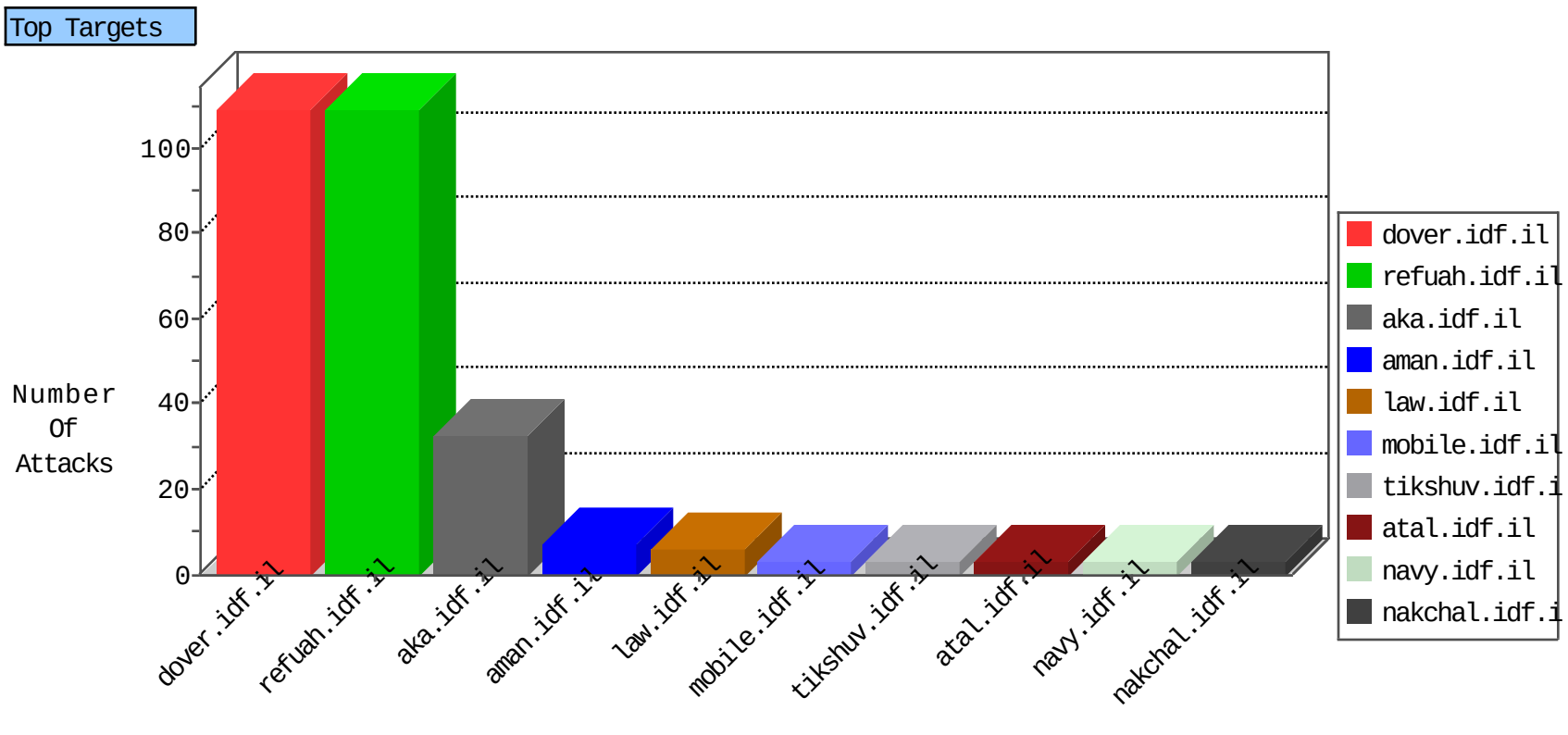
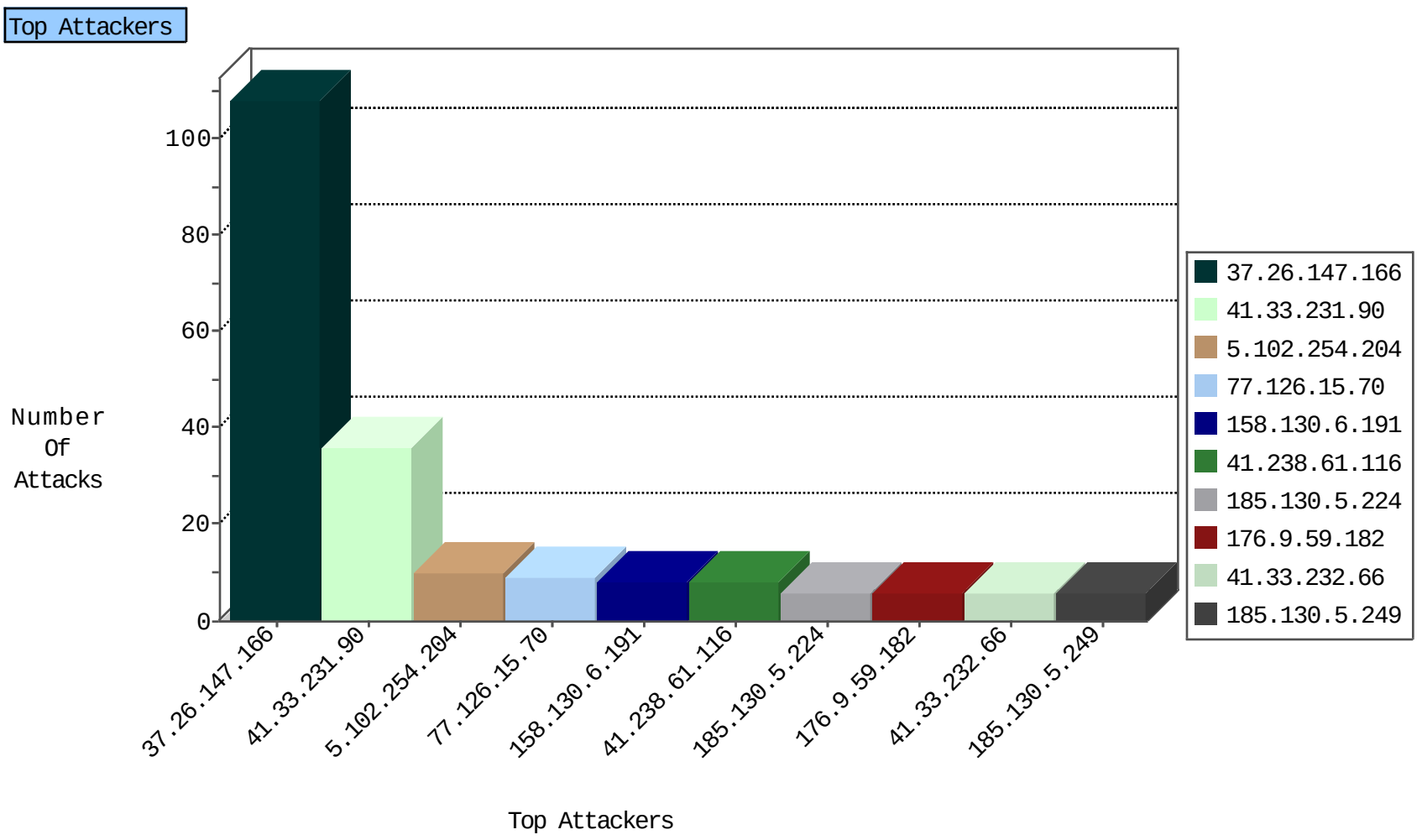
02-11-2016-02:04:06 to 02-11-2016-03:04:06

IDF Under Attack Daily Report





02-11-2016-02:04:06 to 02-11-2016-03:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.166	Israel	147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	41
41.238.61.116	Egypt	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	2
185.130.5.224		147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
151.80.230.228	Italy	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
151.80.230.228	Italy	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
151.80.230.228	Italy	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
151.80.230.228	Italy	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1

02-11-2016-02:04:06 to 02-11-2016-03:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.132	France	147.237.72.156	aman.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-11-2016-02:04:06 to 02-11-2016-03:04:06

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	2
175.6.228.149	147.237.0.35	China	akaws.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
51.254.23.230	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
51.254.23.230	147.237.77.226	United Kingdom	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
51.254.23.230	147.237.77.178	United Kingdom	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.67	147.237.72.156	Turkey	aman.idf.il	ET SCAN NMAP -sS window 1024	1
164.39.11.198	147.237.77.61	United Kingdom	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
51.254.23.230	147.237.77.233	United Kingdom	atal.idf.il	ET SCAN Potential SSH Scan	1
51.254.23.230	147.237.77.179	United Kingdom	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
51.254.23.230	147.237.77.176	United Kingdom	matpash.idf.il	ET SCAN Potential SSH Scan	1

02-11-2016-02:04:06 to 02-11-2016-03:04:06

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
37.26.147.166	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
37.26.147.166	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	21
37.26.147.166	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	9
37.26.147.166	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
77.126.15.70	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
5.102.254.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
5.22.134.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
41.238.61.116	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.210.148.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.73.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.143.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.16.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.18.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.102.254.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
41.238.61.116	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
91.200.12.136	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
197.45.132.185	Egypt	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
184.72.135.223	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
37.26.146.198	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
158.130.6.191	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
203.127.96.220	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.130.5.249		147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
165.91.4.53	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
158.130.6.191	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.150.214.90	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.20.70.114	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.130.5.249		147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
158.130.6.191	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
157.55.12.73	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
203.127.96.220	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.249		147.237.0.35	akaws.idf.il	drop	SAM rule	drop	1
170.20.96.2	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
158.130.6.191	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.179.215.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
203.127.96.219	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
52.6.2.64	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
185.130.5.249		147.237.0.16	my-kosher-kravi.idf.il	drop	SAM rule	drop	1
158.130.6.191	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
157.55.12.73	United States	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
203.127.96.220	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

02-11-2016-02:04:06 to 02-11-2016-03:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.9.59.182	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.9.59.182	Block	5
108.63.106.110	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	2
157.55.39.39	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1
41.129.193.65	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
176.9.59.182	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
157.55.39.113	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
66.249.64.186	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
177.221.41.249	Brazil	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
89.211.78.81	Qatar	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
157.55.39.209	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.209	Block	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20329-he/dover.aspx	Block	1
177.221.41.249	Brazil	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
89.211.78.81	Qatar	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
37.26.147.166	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
165.91.4.53	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
66.249.78.87	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
177.228.5.182	Mexico	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/2063-en/congat.aspx	Block	1
41.129.193.65	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1

02-11-2016-02:04:06 to 02-11-2016-03:04:06