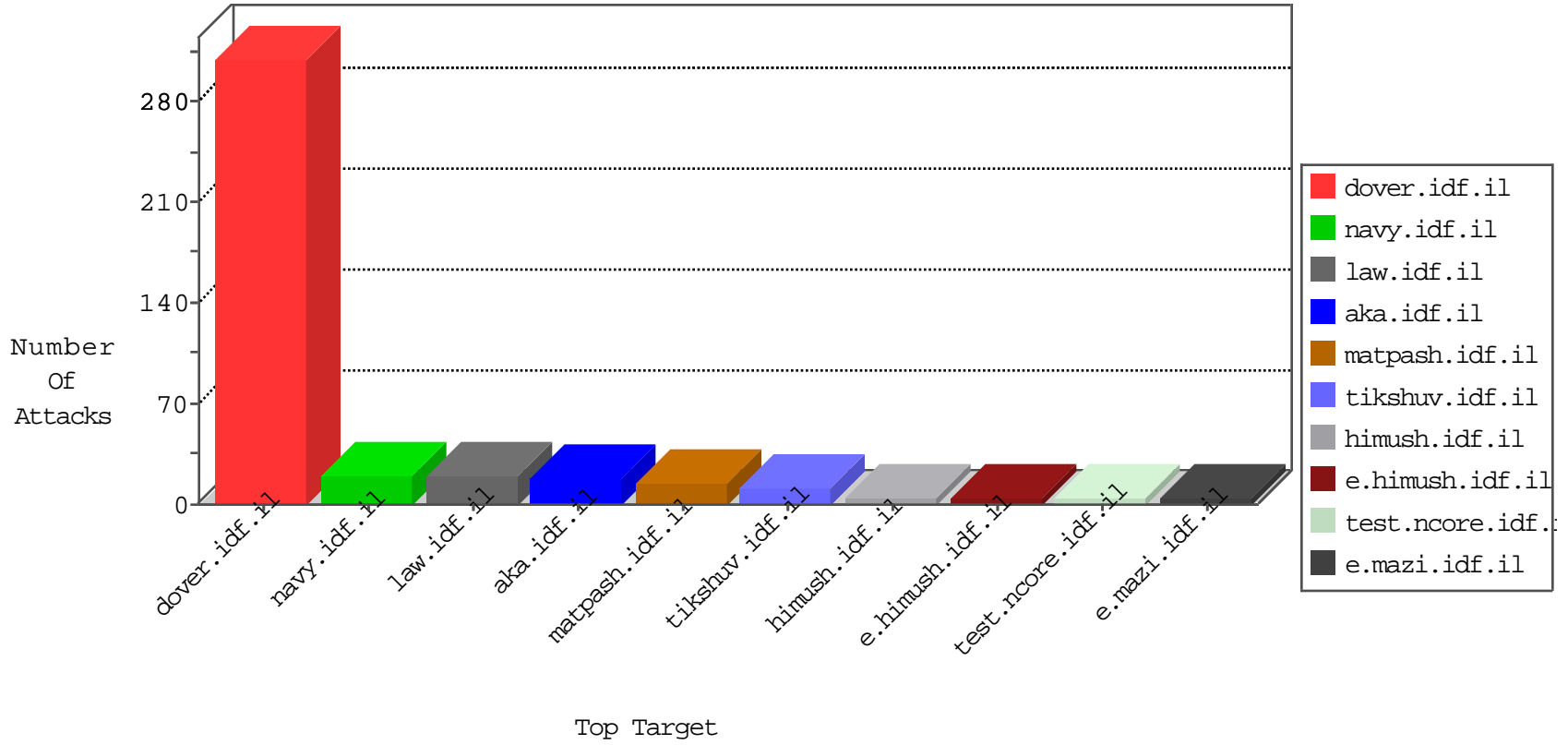


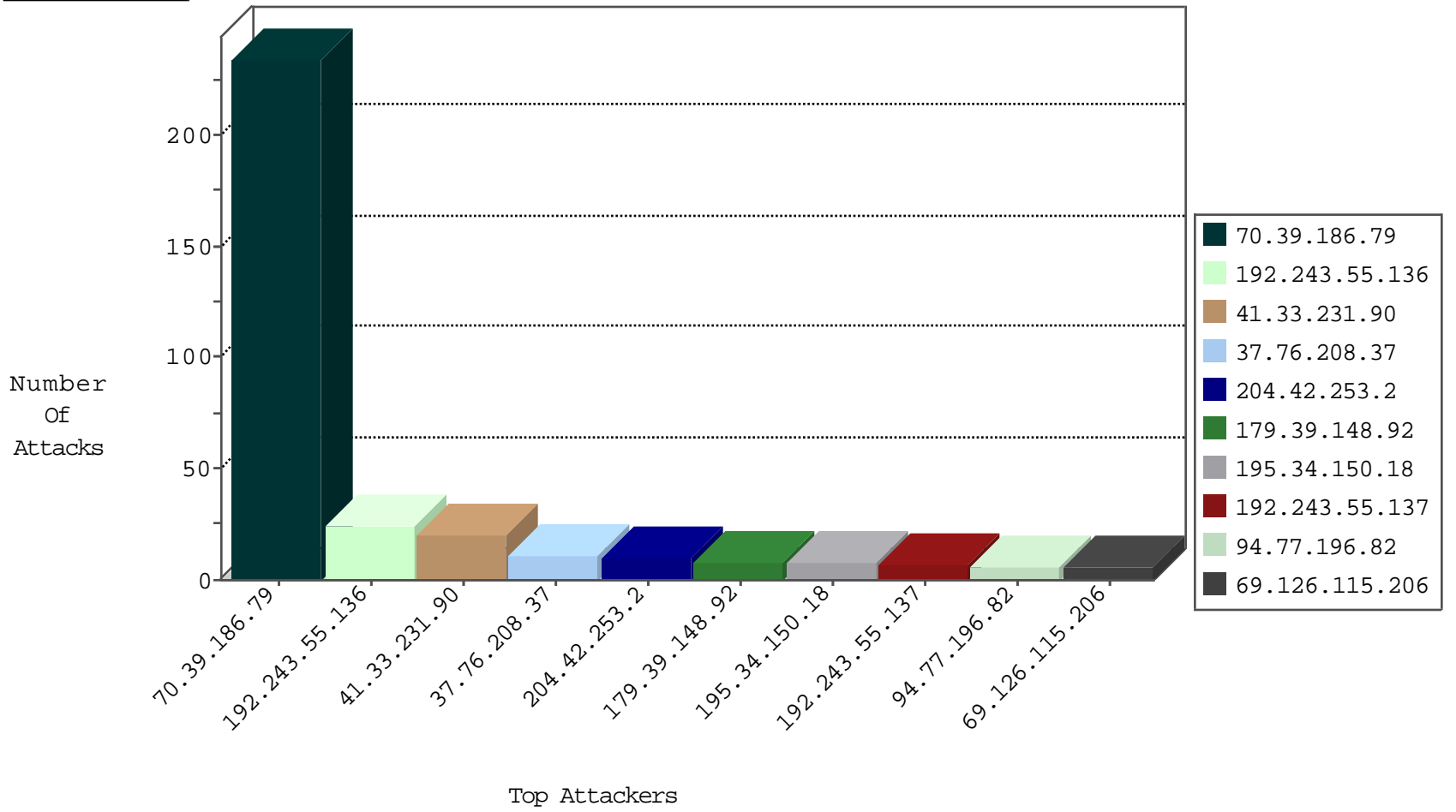
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
183.60.48.25	China	147.237.76.197	e.himush.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
204.42.253.2	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	2
70.39.186.79	Satellite Provider	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
204.42.253.2	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	2
115.239.228.10	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Http	drop	1
185.103.252.5		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.42.225	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
46.121.208.77	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: 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	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
125.67.230.11	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.240.236.119	147.237.76.30	United States	himush.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
185.93.185.246	147.237.77.243		mobile.idf.il	ET SCAN Potential SSH Scan	1
185.93.185.246	147.237.77.179		e.mazi.idf.il	ET SCAN Potential SSH Scan	1
185.93.185.246	147.237.76.42		refuah.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.147	China	chiruch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.193	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
185.93.185.246	147.237.77.227		e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
185.93.185.246	147.237.77.121		e.navy.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.42	China	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
70.39.186.79	Satellite Provider	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	119
70.39.186.79	Satellite Provider	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	113
37.76.208.37	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	11
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
179.39.148.92	Argentina	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
128.69.152.23	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
69.126.115.206	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
217.107.197.109	Russian Federation	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
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
69.126.115.206	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
149.78.47.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
66.249.66.63	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
192.243.55.137	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.85.47	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
192.243.55.137	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.86.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
141.212.122.92	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.188	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.121	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
192.243.55.137	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
180.97.106.37	China	147.237.77.235	sviva.idf.il	drop	SAM rule	drop	1
141.212.122.123	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.115	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.190	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.98	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.122	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.86	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.51	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.97.106.162	China	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
141.212.122.125	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
207.46.13.85	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.116	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.65.214.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1

02-19-2016-03:04:00 to 02-19-2016-04:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.217.88	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
207.46.13.193	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
91.210.147.159	Ukraine	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 91.210.147.159	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
91.210.147.159	Ukraine	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wp-login.php	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
31.201.203.158	Netherlands	147.237.77.74	law.idf.il	PHP Attempt	Block	1
91.210.147.159	Ukraine	147.237.76.86	navy.idf.il	Admin Blocking	Block	1
184.105.247.195	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
31.201.203.158	Netherlands	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
91.210.147.159	Ukraine	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1

02-19-2016-03:04:00 to 02-19-2016-04:04:00