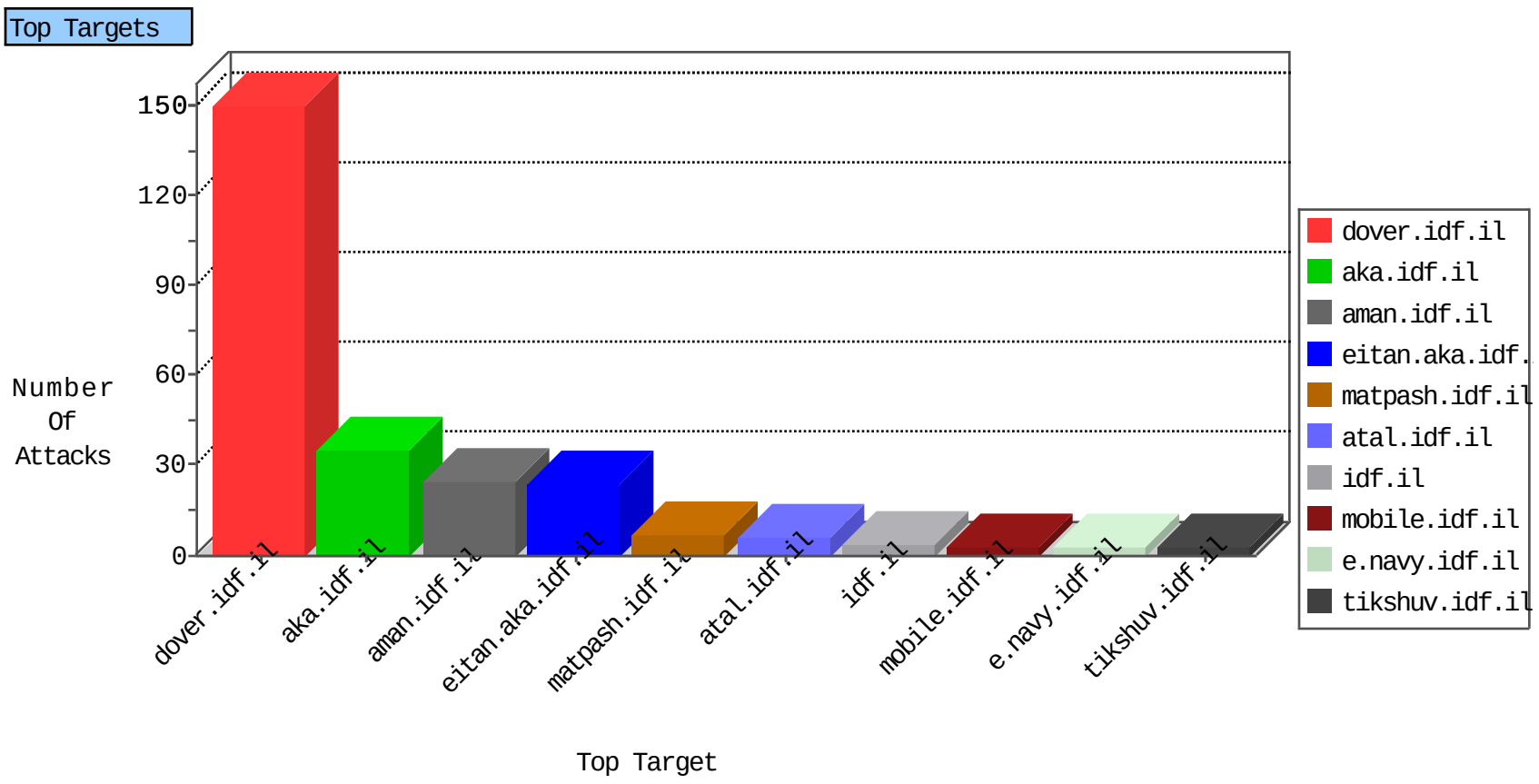
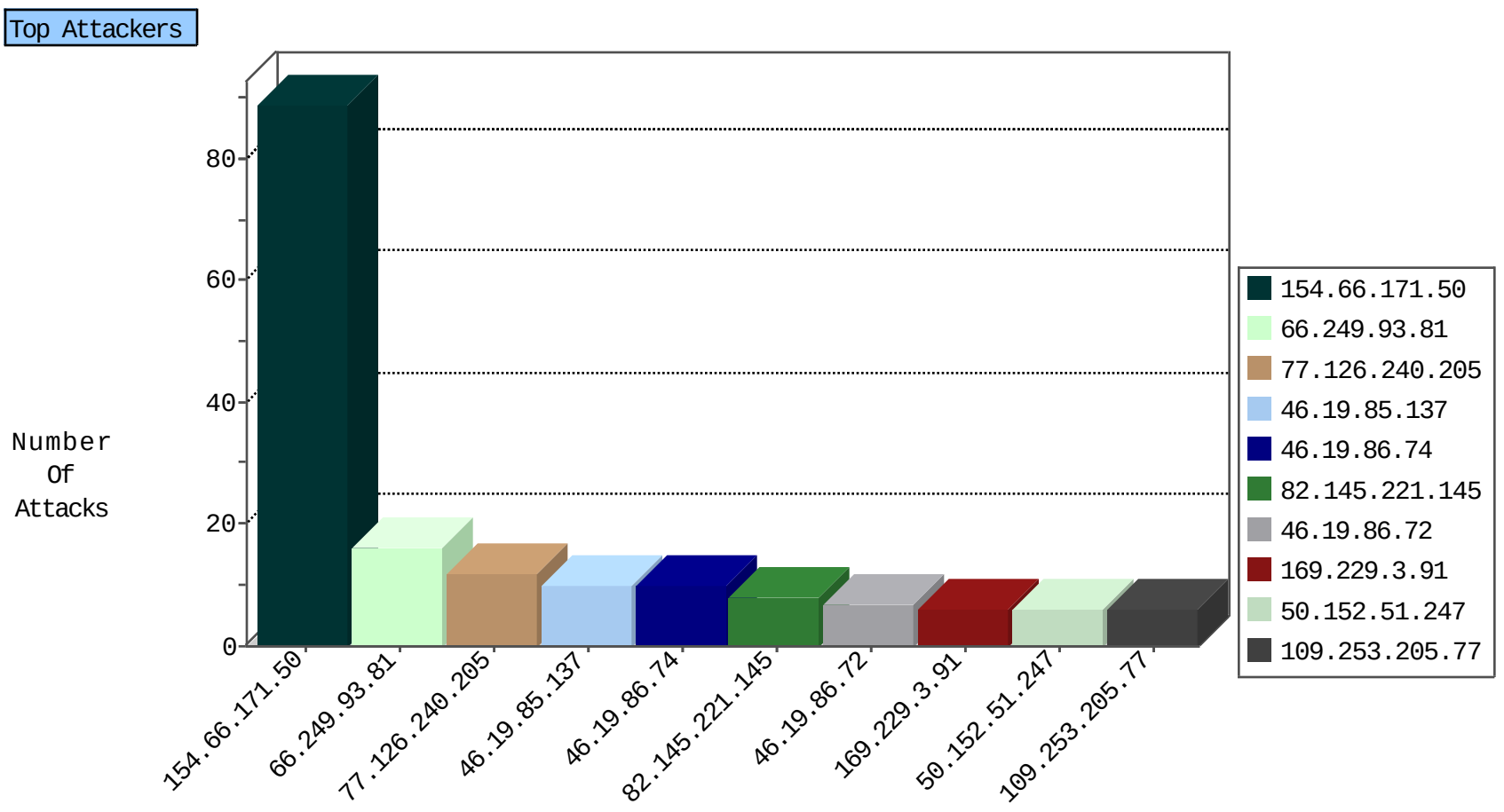
09-21-2016-01:11:46 to 09-21-2016-02:11:46

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-21-2016-01:11:46 to 09-21-2016-02:11:46

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
115.47.12.162	China	147.237.8.24	e.lifestyle.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
45.32.201.228	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
5.206.225.56	Portugal	147.237.76.197	e.himush.idf.il	Black List	drop	1
45.32.205.133	Netherlands	147.237.76.177	ncore.idf.il	Black List	drop	1
45.32.196.8	United States	147.237.76.201	e.atal.idf.il	Black List	drop	1
45.32.205.187	Netherlands	147.237.76.176	test.ncore.idf.il	Black List	drop	1
45.32.201.228	Netherlands	147.237.76.34	yohalan.idf.il	Black List	drop	1

09-21-2016-01:11:46 to 09-21-2016-02:11:46

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2

09-21-2016-01:11:46 to 09-21-2016-02:11:46

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
84.229.70.110	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
66.249.65.157	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
192.151.154.43	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
66.240.213.93	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
192.151.154.43	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -f -sS	1
118.103.126.194	147.237.77.170	Japan	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
116.71.128.85	147.237.77.243	Pakistan	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
115.47.12.162	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
113.182.134.15	147.237.0.200	Vietnam	m4u.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.50	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
208.73.143.36	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
200.98.129.125	147.237.72.156	Brazil	aman.idf.il	ET SCAN Potential SSH Scan	1
66.240.213.93	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
192.151.154.43	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 2048	1
177.200.192.51	147.237.76.198	Brazil	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
118.103.126.194	147.237.76.39	Japan	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
116.71.128.85	147.237.77.235	Pakistan	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
113.248.12.128	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.174.91.29	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
200.98.129.125	147.237.76.42	Brazil	refuah.idf.il	ET SCAN Potential SSH Scan	1

09-21-2016-01:11:46 to 09-21-2016-02:11:46

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
154.66.171.50	Burkina Faso	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
154.66.171.50	Burkina Faso	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
66.249.93.81	Europe	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
154.66.171.50	Burkina Faso	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	11
154.66.171.50	Burkina Faso	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
82.145.221.145	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
109.253.205.77	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
154.66.171.50	Burkina Faso	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
154.66.171.50	Burkina Faso	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
66.249.93.79	Europe	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.126.240.205	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
154.66.171.50	Burkina Faso	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
66.249.64.124	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.109.6.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.76.106	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.109.6.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.86.72	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
2.53.181.177	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
77.126.240.205	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
207.46.13.31	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
50.152.51.247	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
122.56.199.16	New Zealand	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
77.139.64.74	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
162.210.196.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
50.152.51.247	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
131.253.27.185	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.72	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
50.152.51.247	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.86.72	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
70.193.217.6	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
46.183.222.93	Latvia	147.237.77.176	matpash.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
109.64.115.246	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.162	China	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
180.97.106.37	China	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
137.226.113.7	Germany	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
195.60.235.58	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
84.111.39.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
180.97.106.161	China	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
84.108.98.160	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
70.193.217.6	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.183.222.93	Latvia	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
183.184.31.227	China	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-21-2016-01:11:46 to 09-21-2016-02:11:46

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.106	Block	2
157.55.39.242	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
66.249.64.112	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/tutimprahim21122010.aspx	Block	1
77.237.138.202	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized Method HEAD for /	Block	1
2.53.147.111	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
169.229.3.91	United States	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.64.124	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/925-he/chinuch.aspx	Block	1
79.181.130.90	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
66.249.64.93	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
89.138.169.95	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.64.108	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.64.108	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/main/giyus/general.aspx	None	1
93.173.37.19	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.108	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/17102010dohshvuee.aspx	Block	1
68.180.228.238	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1

09-21-2016-01:11:46 to 09-21-2016-02:11:46