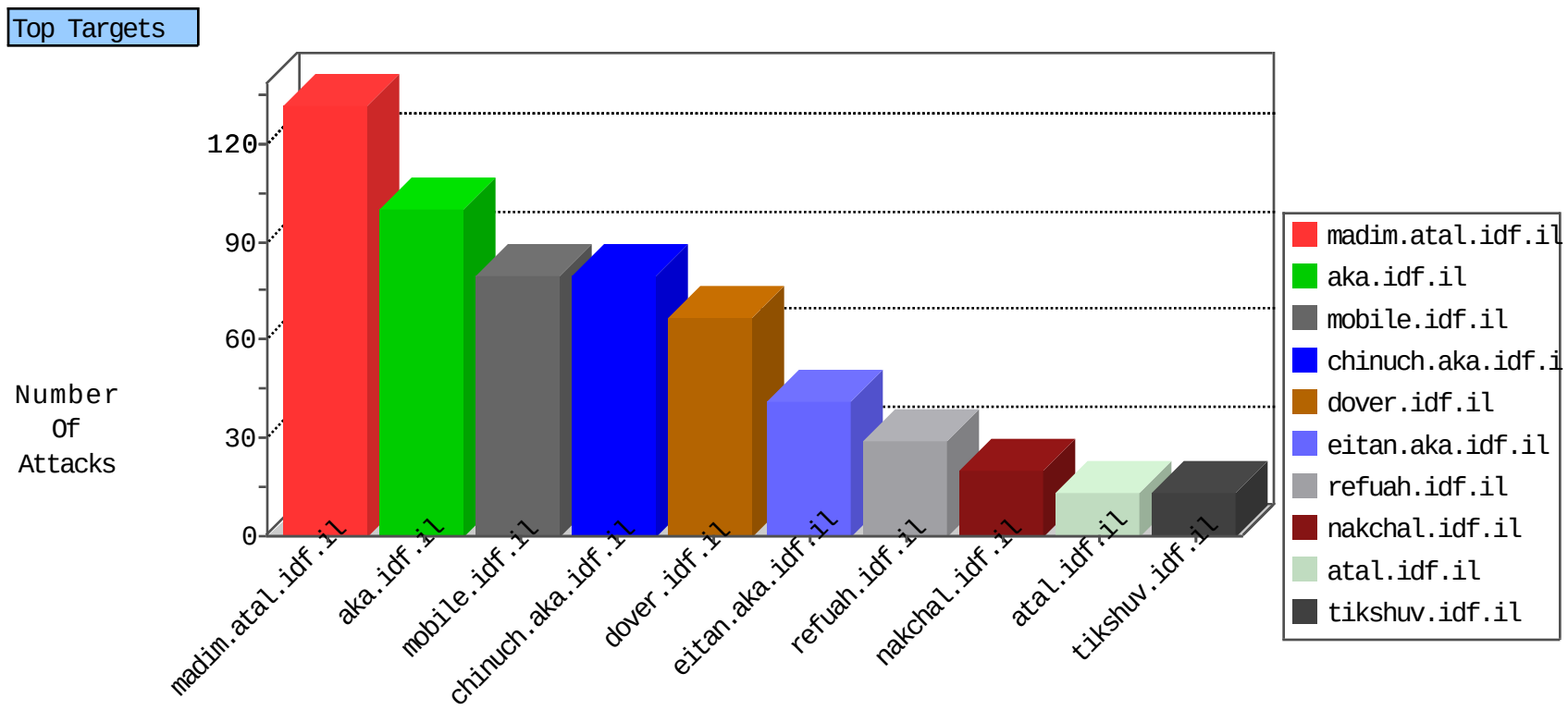
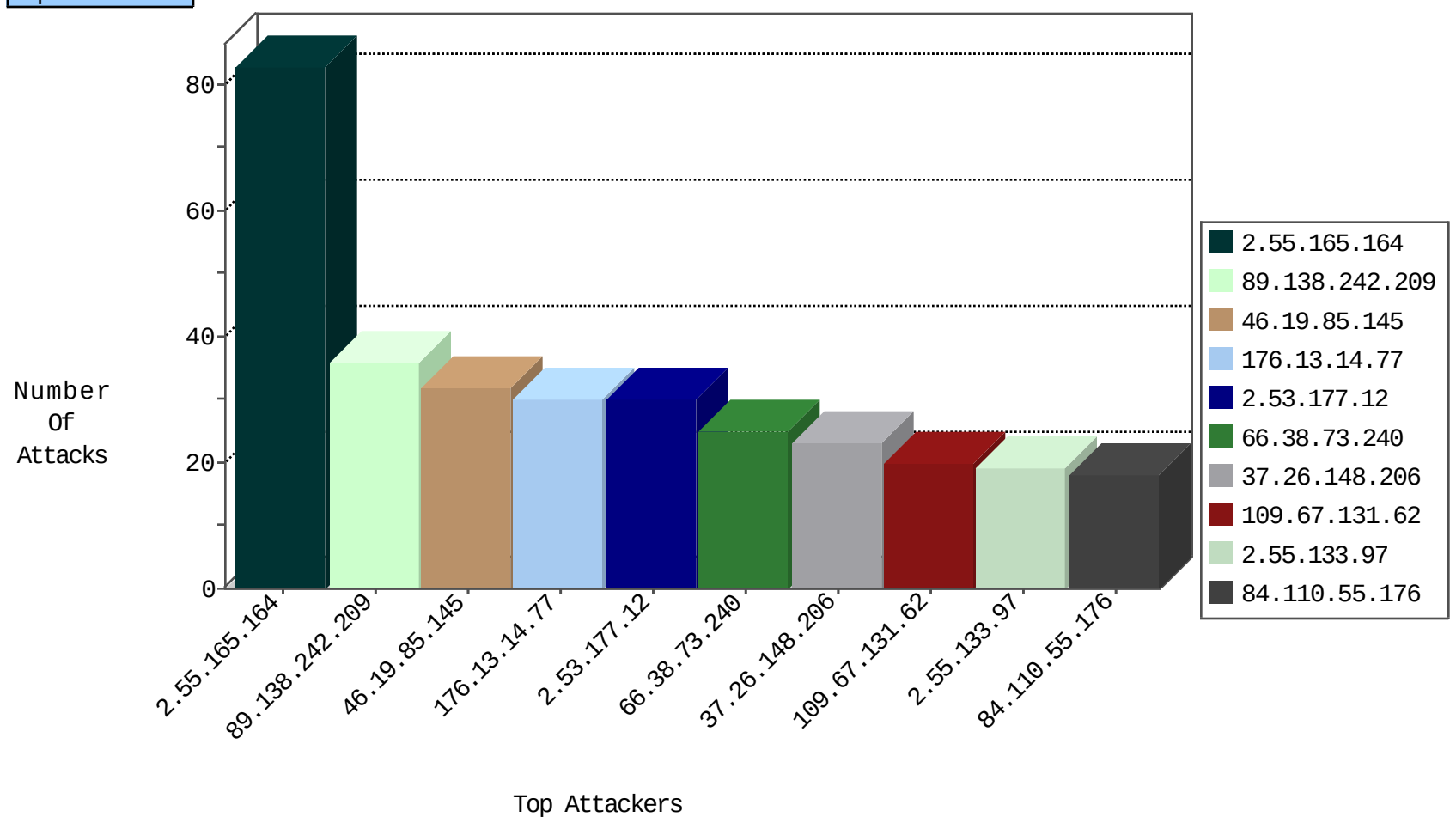
09-27-2016-07:04:01 to 09-27-2016-08:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-27-2016-07:04:01 to 09-27-2016-08:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
104.238.146.180	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1

09-27-2016-07:04:01 to 09-27-2016-08:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
92.238.226.245	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3

09-27-2016-07:04:01 to 09-27-2016-08:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.137	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	3
91.201.236.155	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.155	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
66.249.76.118	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
62.90.11.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
192.223.72.100	147.237.76.39	Bolivia	mobile.meitav.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
45.63.43.107	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
176.53.126.98	147.237.72.156	Turkey	aman.idf.il	ET SCAN NMAP -sS window 1024	1
5.135.90.164	147.237.0.19	France	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
149.255.108.192	147.237.76.38	United Kingdom	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
66.249.93.139	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	1
66.249.93.135	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	1
66.249.76.71	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
58.218.200.137	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
46.19.86.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.93.185.10	147.237.76.176	Ukraine	test.ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
40.114.15.49	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.8.14	United Kingdom	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1

09-27-2016-07:04:01 to 09-27-2016-08:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
89.138.242.209	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.53.177.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
176.13.14.77	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.38.73.240	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
46.19.85.84	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
46.19.85.145	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.145	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
37.142.226.81	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
46.19.85.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.237.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.237.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
37.26.148.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
84.110.55.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
2.55.133.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.221	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.55.133.97	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
172.56.6.33	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
62.0.200.125	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
24.159.6.34	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
2.55.133.97	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
24.159.6.34	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
46.19.86.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
24.159.6.34	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
172.56.6.33	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
37.26.148.206	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence		monitor	4
79.178.32.225	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
172.56.6.33	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
176.13.237.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
2.55.133.97	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.85.36	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.93.81	Europe	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
172.56.6.33	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
37.26.148.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.110.55.176	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
37.26.148.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
50.143.137.1	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
84.110.55.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.20	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.110.55.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.76.30	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.127	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.110.55.176	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
176.13.237.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	2
46.19.85.72	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

09-27-2016-07:04:01 to 09-27-2016-08:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.165.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
109.67.131.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
46.19.86.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
66.249.76.30	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.76.30	Block	6
37.26.147.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.53.167.253	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	3
80.246.137.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
138.134.102.16	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	3
77.124.37.26	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	2
2.55.151.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.138.56	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/default.aspx	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9688-he/refuah.aspx	Block	1
66.249.76.118	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.64.163	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1875	Block	1
5.22.134.245	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9686-he/refuah.aspx	Block	1
52.65.27.248	Australia	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/web-console/serverinfo.jsp	Block	1
66.249.64.166	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1882	Block	1
10.145.70.4		147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
138.134.102.16	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 138.134.102.16	Block	1
54.183.213.28	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/web-console/serverinfo.jsp	Block	1
66.249.66.19	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/m/	Block	1
37.26.147.133	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation searchText in www.refua.atal.idf.il/1467-he/refuah.aspx	Block	1
138.134.102.16	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
66.249.76.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1879	Block	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
66.249.64.85	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/mobile/	Block	1

09-27-2016-07:04:01 to 09-27-2016-08:04:01