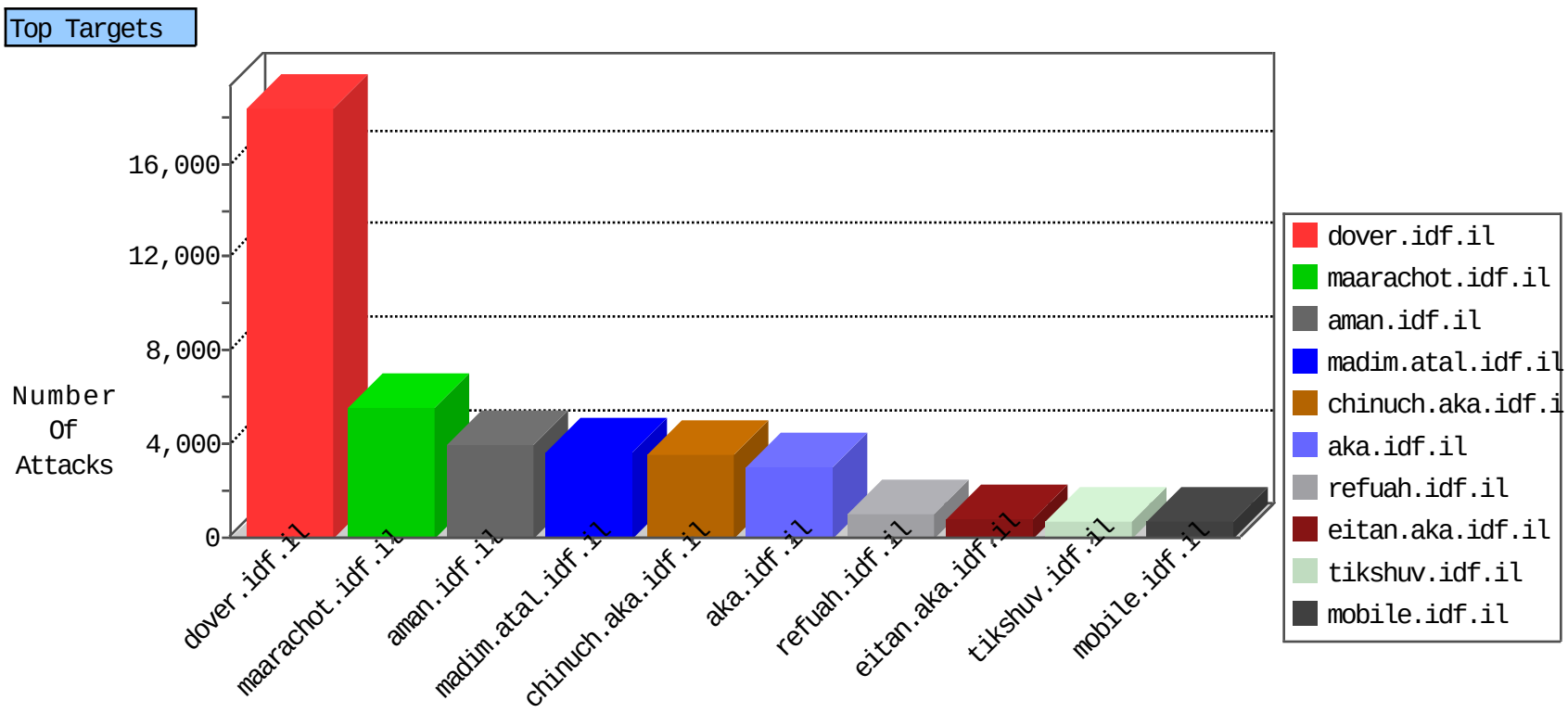
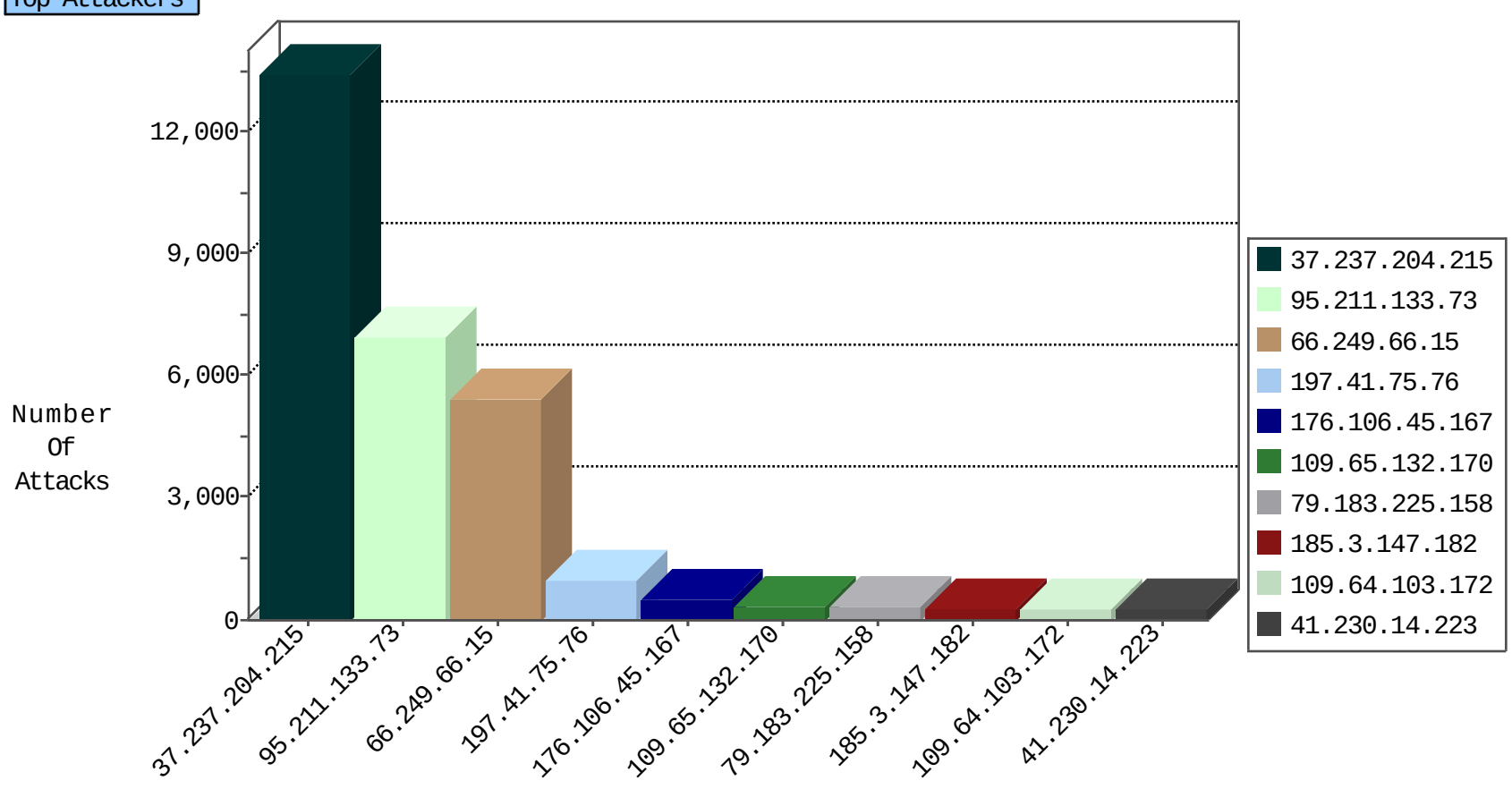
03-05-2016 to 03-06-2016

IDF Under Attack
Daily Report

Top Targets



Top Attackers



03-05-2016 to 03-06-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.41.75.76	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	954
176.106.45.167	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	432
37.237.204.215	Iraq	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	304
197.117.70.37	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	226
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	111
176.106.45.167	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	42
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	25
37.237.204.215	Iraq	147.237.77.216	dover.idf.il	DOS-WEB-HOIC-HTTP-80-snc	dest-reset	21
82.145.220.82	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
82.145.216.219	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
82.145.218.194	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
212.199.241.250	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	7
77.127.14.31	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	7
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
82.145.223.150	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
104.172.112.17	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	5
82.145.211.8	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
82.145.216.93	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
82.145.219.60	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4
149.78.148.181	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	3
37.237.204.215	Iraq	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
176.77.33.24	Russian Federation	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
134.147.203.115	Germany	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	2
37.237.204.215	Iraq	147.237.77.216	dover.idf.il	DOS-HOIC-TCP-80-gbo	dest-reset	2
134.147.203.115	Germany	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	2
183.60.48.25	China	147.237.0.19	madim.atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
107.208.122.143	United States	147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	2
61.160.6.152	China	147.237.0.15	kosher-kravi.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
176.77.33.24	Russian Federation	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
85.64.189.233	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	2
134.147.203.115	Germany	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	2
111.118.160.177	Australia	147.237.0.16	my-kosher-kravi.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
134.147.203.115	Germany	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	2
115.239.228.10	China	147.237.0.17	m.my-kosher-kravi.idf.il	JLM_Under_Attack_Con_Http	drop	2
46.117.248.198	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	2
134.147.203.115	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	2
52.31.84.220	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	2
181.199.135.122	Peru	147.237.0.35	akaws.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
115.239.228.10	China	147.237.0.15	kosher-kravi.idf.il	JLM_Under_Attack_Con_Http	drop	2
37.237.204.215	Iraq	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
134.147.203.115	Germany	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	2

03-05-2016 to 03-06-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.237.204.215	Iraq	147.237.77.216	dover.idf.il	20034: HTTP: HOIC Denial-of-Service Tool Usage	Block	81
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	24
37.142.236.219	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	20
123.126.113.162	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	19
46.121.214.54	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
79.176.144.42	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	13
79.182.151.228	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
85.64.181.168	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
181.177.20.14	Argentina	147.237.0.34	tikshuv.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	10
31.154.163.198	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
176.13.19.240	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
79.176.162.120	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
82.80.178.57	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
77.125.89.0	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.181.14.13	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
85.65.20.84	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.121.87.162	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
109.64.41.47	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
109.65.108.217	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
79.179.143.83	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
95.86.117.109	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
5.29.107.7	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
80.246.130.27	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
176.228.142.171	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
109.66.2.249	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
159.122.255.247	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
5.29.119.174	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
159.122.255.247	Netherlands	147.237.0.19	madim.atal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
37.26.149.188	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
79.180.189.209	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
79.178.25.73	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
94.230.95.203	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
5.29.75.74	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
84.229.34.220	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
2.54.45.144	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.121.252.68	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
195.154.185.20	France	147.237.77.170	maarachot.idf.il	C1000074: HTTP: majestic bot	Block	4
46.120.39.226	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
109.67.43.105	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
49.246.230.40	China	147.237.77.74	law.idf.il	8479: HTTP: Suspicious HTTP Request	Block	4
149.88.153.63	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
84.228.86.248	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
178.12.105.6	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	3
31.154.249.157	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3

03-05-2016 to 03-06-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	5437
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	96
41.191.97.51	147.237.77.216	Ghana	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	6
218.246.0.97	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 1024	3
213.136.91.26	147.237.76.31	Germany	nakchal.idf.il	ET SCAN Potential SSH Scan	3
66.249.64.233	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
218.57.11.7	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
209.126.116.147	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
66.102.9.17	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
80.246.130.69	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
209.126.116.147	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
59.45.79.117	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	2
218.246.0.97	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	2
213.136.91.26	147.237.77.234	Germany	halag.idf.il	ET SCAN Potential SSH Scan	2
209.126.116.147	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	2
213.136.91.26	147.237.77.179	Germany	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
66.249.79.78	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sA (2)	2
213.136.91.26	147.237.8.24	Germany	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
66.249.65.14	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sA (2)	2
218.57.11.7	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	2
5.29.189.176	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
181.177.20.14	147.237.0.34	Argentina	tikshuv.idf.il	ET WEB_SERVER Muieblackcat scanner	2
66.249.64.200	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
37.26.149.166	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
132.252.173.4	147.237.77.216	Germany	dover.idf.il	GPL SCAN nmap TCP	2
213.136.91.26	147.237.0.15	Germany	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
66.102.9.13	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
213.136.91.26	147.237.76.34	Germany	yohalan.idf.il	ET SCAN Potential SSH Scan	2
192.198.151.37	147.237.72.167	Europe	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
213.136.91.26	147.237.77.216	Germany	dover.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.91	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
94.102.48.193	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.66.36	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	2
218.57.11.7	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
213.136.91.26	147.237.8.14	Germany	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
199.101.186.245	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
13.75.95.104	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
182.18.143.75	147.237.76.197	India	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
113.176.83.10	147.237.0.19	Vietnam	madim.atal.idf.il	WEB-CGI redirect access	1
89.248.172.140	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
210.178.74.167	147.237.0.34	Korea, Republic of	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
52.27.12.37	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
187.150.170.245	147.237.76.30	Mexico	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
159.122.220.108	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
104.192.0.19	147.237.72.156	United States	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
213.136.91.26	147.237.76.200	Germany	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
107.150.36.36	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.77.179		e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
37.139.27.231	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1

03-05-2016 to 03-06-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.237.204.215	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12007
95.211.133.73	Netherlands	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2763
95.211.133.73	Netherlands	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2331
95.211.133.73	Netherlands	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	1131
95.211.133.73	Netherlands	147.237.72.156	aman.idf.il	SYN Attack		reject	702
37.237.204.215	Iraq	147.237.77.216	dover.idf.il	drop		drop	574
109.64.103.172	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	273
185.3.147.182	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	258
85.64.218.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	204
37.237.204.215	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	185
79.177.57.196	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	165
2.54.136.49	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	147
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	144
195.154.250.49	France	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	131
37.237.204.215	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	131
87.69.35.157	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	104
213.57.233.67	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	92
37.237.204.215	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	80
176.13.4.21	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
132.74.151.249	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
176.77.33.24	Russian Federation	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	62
89.139.162.197	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	55
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	51
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	51
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	51
79.181.173.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
79.181.64.160	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	47
109.67.248.43	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	46
93.173.224.145	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	46
176.13.18.32	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	44
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	44
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	43
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	43
109.253.138.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
109.253.138.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	41
46.19.86.27	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
2.54.172.142	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	39
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	38
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	38
188.139.228.62	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
188.139.228.62	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	35
46.19.85.52	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
213.57.96.78	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
66.249.93.91	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	33
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	33

03-05-2016 to 03-06-2016

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	32

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.132.170	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	347
79.183.225.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	340
2.54.42.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	241
5.29.167.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	186
46.19.85.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	184
183.60.244.44	China	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 183.60.244.44	Block	181
176.13.18.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	173
46.19.86.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	171
84.111.104.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	164
2.52.24.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	149
2.54.52.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	121
46.19.85.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
79.182.179.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
46.19.86.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	99
2.52.184.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	91
46.19.86.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
77.127.23.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
37.26.149.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
109.67.173.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
2.54.171.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
2.54.164.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
85.65.116.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
2.52.164.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
46.19.86.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
192.116.108.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
109.253.220.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
37.26.147.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
46.116.159.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	29
2.52.164.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
109.67.124.76	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	28
183.60.244.44	China	147.237.72.156	aman.idf.il	Multiple Admin Blocking from 183.60.244.44	Block	27
46.19.86.83	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.19.86.83	Block	26
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	25
85.64.109.198	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.64.109.198	Block	20
80.179.96.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
183.60.244.44	China	147.237.72.156	aman.idf.il	PHP Attempt	Block	19
217.132.156.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	15
41.230.14.223	Tunisia	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 41.230.14.223	Block	13
41.230.14.223	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	13
109.253.138.219	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	13
109.253.138.111	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	12
41.230.14.223	Tunisia	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	12
41.230.14.223	Tunisia	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	10
5.102.195.114	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtStreet in madim.atal.idf.il/1088-he/meretz.aspx	Block	10
195.60.232.57	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 195.60.232.57	Block	9
176.13.4.21	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
37.46.39.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
2.54.16.89	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	8

03-05-2016 to 03-06-2016