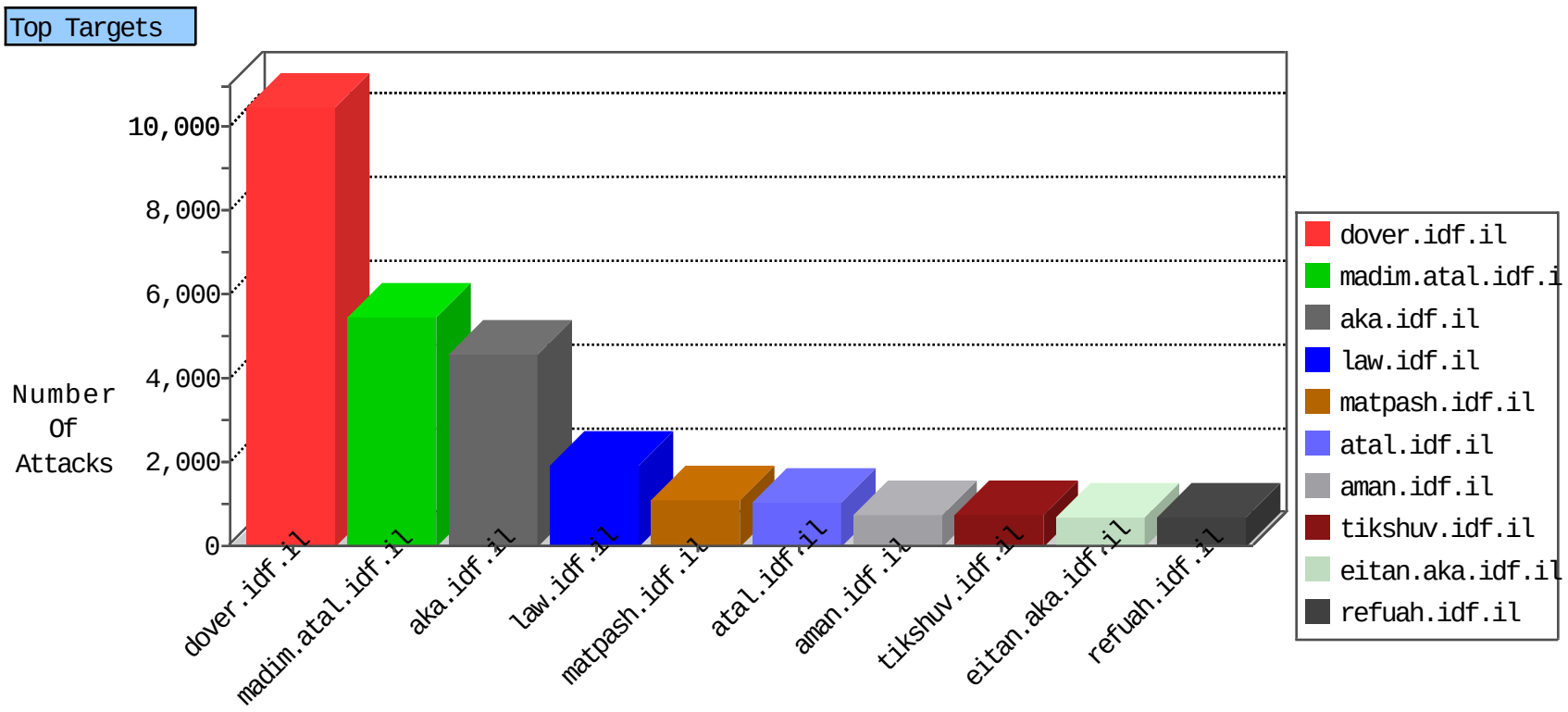
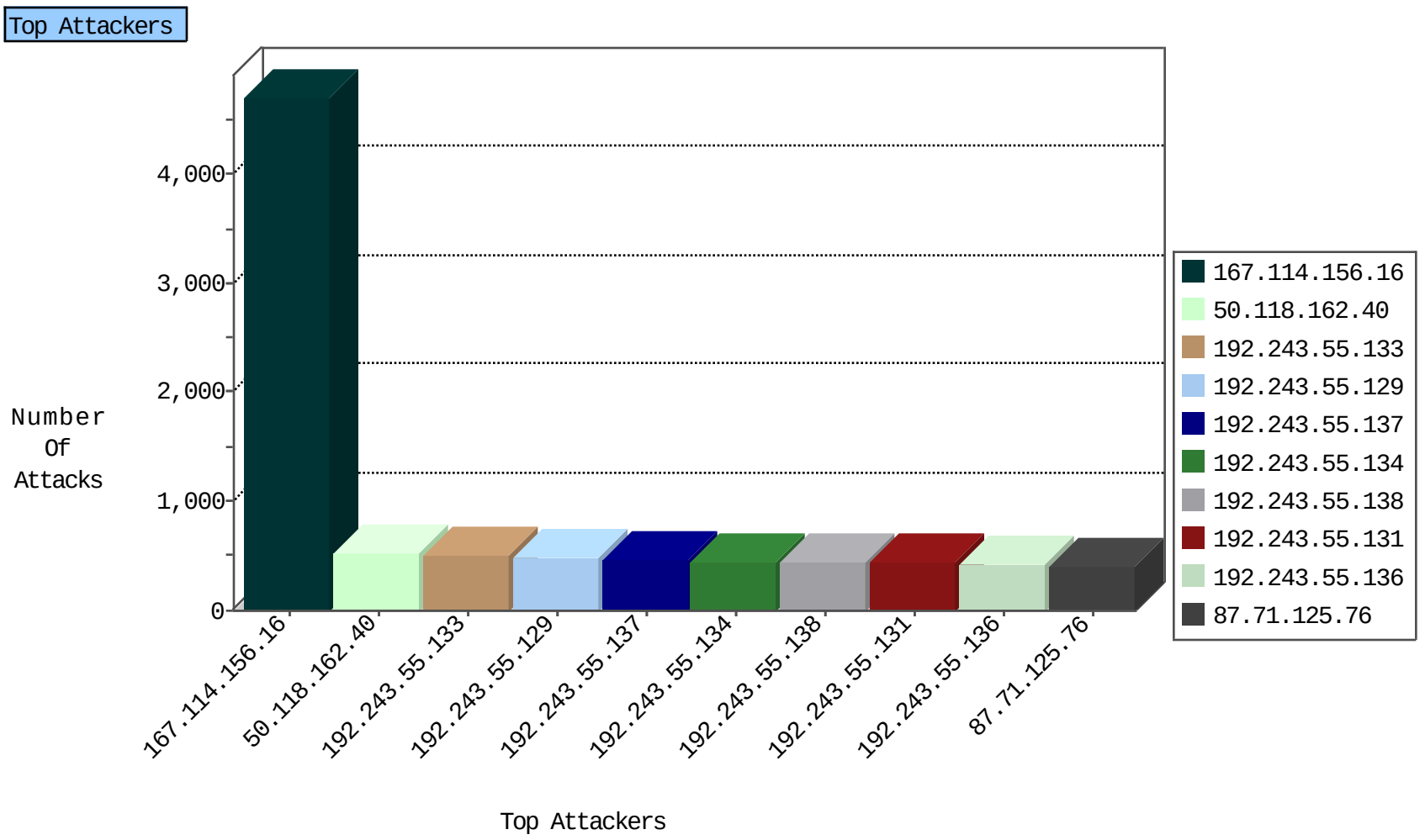
03-10-2016 to 03-11-2016

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-10-2016 to 03-11-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	25173
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	331
46.32.214.63	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SQL-Inj-Pang-GMSSQLInt1	dest-reset	180
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	158
2.52.149.49	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	63
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	37
196.200.156.104	Morocco	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-product3	dest-reset	24
79.183.98.143	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	21
82.145.208.76	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	21
82.145.211.126	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	15
41.248.100.203	Morocco	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-product3	dest-reset	15
37.26.148.188	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
82.145.218.138	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	12
105.156.146.186	Morocco	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-product3	dest-reset	12
41.142.144.45	Morocco	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-product3	dest-reset	11
50.118.162.40	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
82.145.210.236	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
82.145.220.185	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
41.140.126.30	Morocco	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-product3	dest-reset	7
82.145.218.34	Europe	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	6
8.37.231.91	Anonymous Proxy	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	6
79.177.116.56	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	6
50.118.162.211	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
82.145.217.244	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
82.145.221.141	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
82.145.216.142	Europe	147.237.72.166	aka.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
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
8.37.231.91	Anonymous Proxy	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	4
89.248.160.132	Netherlands	147.237.77.205	prisha.idf.il	block-sp-traf1	forward	4
81.218.8.34	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
190.151.180.28	El Salvador	147.237.76.148	gqcenter.aka.idf.il	L4 Source or Dest Port Zero	drop	3
66.249.64.233	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
80.70.128.129	Israel	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	3
41.137.23.30	Morocco	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	3
82.145.217.21	Europe	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	3
70.39.186.127	Satellite Provider	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
81.218.8.34	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
66.249.64.190	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	3
70.39.186.127	Satellite Provider	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
89.248.160.132	Netherlands	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	2
89.248.160.132	Netherlands	147.237.77.233	atal.idf.il	block-sp-traf1	forward	2
82.145.222.245	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	2
89.248.160.132	Netherlands	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
119.93.47.186	Philippines	147.237.0.200	m4u.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
221.0.95.227	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	2
89.248.160.132	Netherlands	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	2
89.155.108.86	Portugal	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2

03-10-2016 to 03-11-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	36
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	24
85.65.6.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	24
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	23
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	23
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	23
109.65.202.39	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	20
217.194.196.5	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	19
123.126.113.163	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	19
84.109.32.144	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
212.143.240.134	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
87.71.19.141	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
79.181.171.86	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
82.166.198.189	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
79.177.118.182	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
79.182.246.169	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
46.19.85.152	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
2.52.149.24	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
109.67.222.64	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
109.64.173.249	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
79.183.211.18	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
132.72.228.215	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
62.219.120.45	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
5.29.120.176	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.181.56.133	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
5.29.127.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
132.66.61.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
185.3.144.8	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
2.54.16.180	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
199.58.86.211	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	6
192.118.12.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
87.71.37.242	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
176.13.12.107	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
66.249.79.234	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
80.246.133.82	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
109.64.125.21	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
109.64.186.91	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
176.13.5.251	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
84.108.245.193	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.19.86.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
178.63.18.196	Germany	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
31.154.34.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
109.65.213.98	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
64.87.23.55	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
151.80.31.152	Italy	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	4
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
82.166.180.116	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4

03-10-2016 to 03-11-2016

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	68
95.86.127.108	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	8
178.63.18.196	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	6
209.173.241.141	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	6
64.87.23.55	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
212.199.57.193	147.237.72.166	Israel	aka.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
46.32.214.63	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SQL 1 = 1 - possible sql injection attempt	4
80.246.136.27	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	4
212.76.97.178	147.237.77.216	Israel	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
66.249.93.243	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	3
93.189.26.18	147.237.0.35	Austria	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
66.102.9.71	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	2
173.166.65.97	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.32	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
122.227.180.99	147.237.76.198	China	e.yohalan.idf.il	GPL SCAN nmap TCP	2
89.139.40.244	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
80.246.133.111	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.102.6.243	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
66.249.93.128	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sA (2)	2
66.249.79.43	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
37.187.152.205	147.237.77.74	France	law.idf.il	Tehila - Perl LWP with fake user agent	2
93.189.26.18	147.237.8.45	Austria	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	2
80.246.136.103	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
202.71.25.29	147.237.8.27	India	e.madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
46.19.85.202	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.36	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
109.253.141.39	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.251.80	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.57.11.7	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
66.249.64.50	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
192.243.55.136	147.237.77.216	Dominica	dover.idf.il	portscan: TCP Distributed Portscan	1
23.96.109.87	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
169.54.233.116	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.43.201.119	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.207.135.64	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
83.130.105.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.99.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.157	147.237.77.19		law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.152.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.66.54.252	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
221.203.142.131	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
79.178.57.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.172.204	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
178.62.94.12	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.156	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.36	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
109.253.129.80	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

03-10-2016 to 03-11-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
50.118.162.40	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	489
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	172
212.179.61.123	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	116
37.26.146.250	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	111
79.176.34.80	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	91
151.66.105.255	Italy	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	88
31.168.3.26	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	82
79.179.148.55	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	80
192.116.55.97	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
79.181.114.234	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	75
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	69
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
212.179.48.36	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	66
77.125.77.132	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	63
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	62
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	61
176.13.13.156	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
62.219.137.44	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	59
80.246.133.127	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	59
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	58
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	58
212.29.224.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	57
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	57
2.54.131.130	Israel	147.237.72.156	aman.idf.il	SYN Attack		reject	57
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	56
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	55
81.4.163.106	Cyprus	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	54
31.168.147.187	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	53
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	51
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	51
109.253.222.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	49
2.54.131.130	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	48
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	48
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	47
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	45
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	44
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	43
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	43
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	43
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	42
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	41
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	41

03-10-2016 to 03-11-2016

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	41

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.71.125.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	398
2.54.163.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	262
46.19.85.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	257
46.19.86.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	215
80.246.136.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	184
109.253.216.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	173
46.19.85.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	168
46.19.85.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	160
2.52.43.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	153
46.19.85.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	148
2.52.10.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	146
109.253.130.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	120
2.54.183.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
109.64.225.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
213.57.164.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
46.19.85.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
109.253.141.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	105
109.253.144.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
46.19.85.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	98
109.253.193.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
109.253.135.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	95
62.219.99.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	94
80.246.136.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	94
109.253.218.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
2.54.24.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
37.26.149.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
80.246.136.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Automated Vulnerability Scanning V1	Block	73
176.13.16.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
37.26.149.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
109.253.203.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
46.19.85.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
2.54.166.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
37.26.146.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
176.13.13.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
176.13.12.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
46.19.86.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
2.54.24.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
173.208.136.170	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 173.208.136.170	Block	40
46.19.85.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
80.246.136.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
176.13.8.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
109.253.147.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
46.19.86.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
80.246.137.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
2.54.13.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
84.228.108.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
109.253.146.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25

03-10-2016 to 03-11-2016