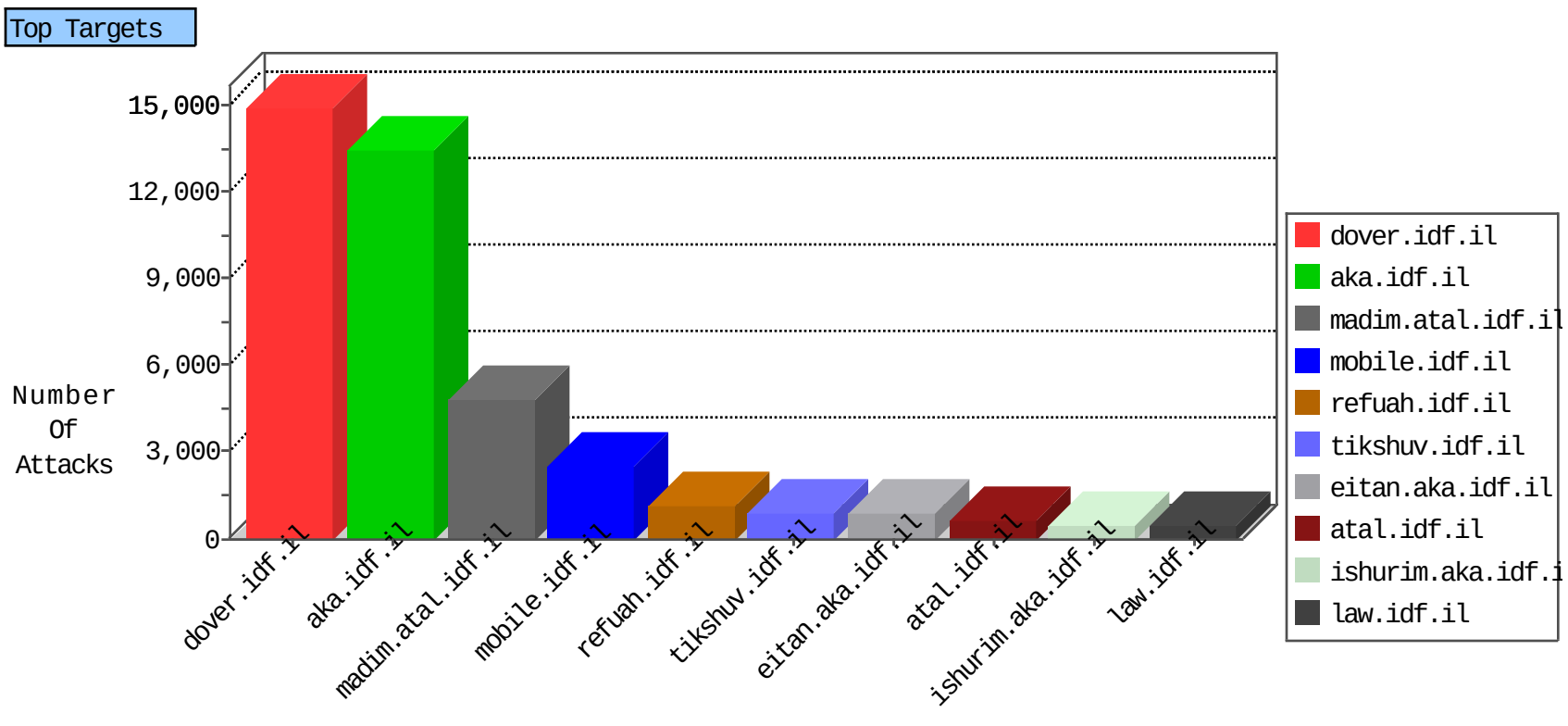
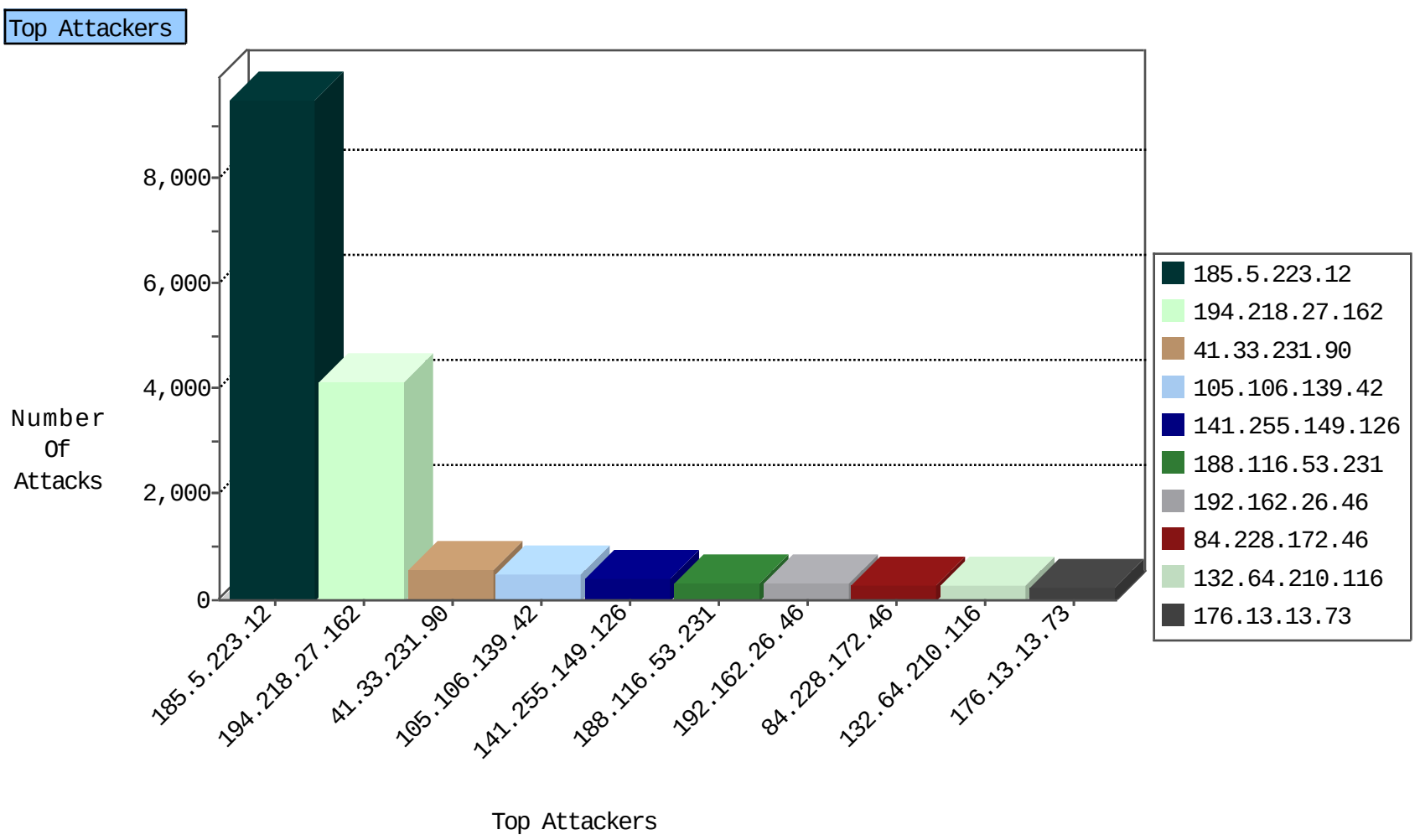
03-01-2016 to 03-02-2016

IDF Under Attack
Daily Report

Top Targets



Top Attackers



03-01-2016 to 03-02-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.5.223.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	8834
185.5.223.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3934
41.143.49.62	Morocco	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	1258
141.255.149.126	Netherlands	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1000
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	898
185.5.223.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	283
141.255.149.126	Netherlands	147.237.77.216	dover.idf.il	DOS-HTTP-torshammer	dest-reset	256
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	177
105.106.139.42	Algeria	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	161
66.249.66.105	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	139
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
46.244.64.164	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	48
41.143.49.62	Morocco	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	47
82.145.216.133	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	25
82.145.209.76	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	22
82.145.218.83	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	19
82.145.216.200	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	15
82.145.218.194	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	12
84.111.112.234	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	12
82.145.218.194	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	12
84.111.112.234	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	12
192.114.38.121	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	9
217.26.171.188	Moldova, Republic of	147.237.77.176	matpash.idf.il	L4 Source or Dest Port Zero	drop	8
82.145.211.18	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
209.126.122.20	United States	147.237.0.33	idf.il	Block_Udp_All_Nets	drop	6
2.54.164.240	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
109.65.181.46	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
79.177.6.20	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
37.142.134.111	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
82.145.210.189	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
209.126.122.20	United States	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	5
217.26.171.188	Moldova, Republic of	147.237.76.176	test.ncore.idf.il	L4 Source or Dest Port Zero	drop	4
185.103.252.5		147.237.77.178	e.matpash.idf.il	Block_Udp_All_Nets	drop	4
185.103.252.5		147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	4
209.126.122.20	United States	147.237.77.212	e.dover.idf.il	Block_Udp_All_Nets	drop	4
185.103.252.5		147.237.8.50	e.tikshuv.idf.il	Block_Udp_All_Nets	drop	4
31.154.94.18	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
31.168.133.226	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
105.106.139.42	Algeria	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
212.179.64.162	Israel	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	3
37.232.10.242	Georgia	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3
212.25.121.195	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
209.126.122.20	United States	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	3
79.181.110.220	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.10	China	147.237.0.35	akaws.idf.il	JLM_Under_Attack_Con_Http	drop	2
85.130.223.95	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
113.53.135.63	Thailand	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
209.126.122.20	United States	147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2

03-01-2016 to 03-02-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.243.118	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	32
46.120.38.35	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	26
109.65.109.249	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	22
106.38.241.107	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	22
61.135.189.110	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	20
37.26.149.240	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
69.30.214.46	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	16
89.138.83.19	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
84.109.18.197	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
85.250.93.194	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
91.231.192.149	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
192.116.55.245	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	13
194.114.146.227	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
188.116.53.231	Poland	147.237.76.200	eitan.aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	12
188.116.53.231	Poland	147.237.76.200	eitan.aka.idf.il	22095: HTTP: Joomla Image Manager folderRename Security Bypass Vulnerability	Block	12
192.118.73.46	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
212.150.189.2	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
31.168.10.91	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
84.109.181.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
79.178.217.6	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
82.80.193.236	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
79.176.30.9	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.67.132.203	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.19.86.56	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
81.218.135.170	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
87.71.72.103	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
185.3.147.144	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.64.5.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
84.111.28.11	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
77.125.98.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
212.116.184.161	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.19.85.41	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.64.125.249	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
94.159.153.82	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
89.139.129.204	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
149.88.88.199	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
188.120.151.217	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
212.199.112.144	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
31.154.94.73	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
173.234.153.122	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	6
217.227.76.195	Germany	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
80.246.130.99	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
2.54.173.223	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
109.253.205.238	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
109.64.85.135	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
109.66.166.47	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
84.228.28.56	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
159.122.222.119	Netherlands	147.237.0.34	tikshuv.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
159.122.222.119	Netherlands	147.237.0.15	kosher-kravi.idf.i	20086: HTTP: Muieblackcat Security Scanner	Block	5

03-01-2016 to 03-02-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
188.116.53.231	147.237.76.200	Poland	eitan.aka.idf.il	Tehila - Perl LWP with fake user agent	76
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	65
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	65
188.116.53.231	147.237.76.200	Poland	eitan.aka.idf.il	SERVER-WEBAPP Mambo upload.php access	40
66.249.66.184	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	26
80.246.133.57	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	21
2.54.155.161	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
37.162.6.255	147.237.76.86	France	navy.idf.il	ET SCAN NMAP -sA (2)	4
66.249.69.26	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	4
84.108.36.159	147.237.77.216	Israel	dover.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	3
212.179.21.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	3
14.139.220.90	147.237.76.199	India	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
2.54.11.181	147.237.77.243	Israel	mobile.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	2
14.139.220.90	147.237.76.38	India	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
185.99.32.3	147.237.76.30		himush.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.43	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.81.196	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
80.246.130.85	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
218.246.0.97	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
193.106.54.36	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.66.107	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
212.235.98.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
37.142.192.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
218.246.0.97	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
93.173.36.31	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
185.99.32.3	147.237.76.86		navy.idf.il	ET SCAN NMAP -sA (2)	2
109.67.28.170	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
14.139.220.90	147.237.76.31	India	nakchal.idf.il	ET SCAN Potential SSH Scan	2
128.30.52.96	147.237.76.86	United States	navy.idf.il	Tehila - Perl LWP with fake user agent	2
218.57.11.7	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	2
31.154.94.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
37.26.147.222	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
89.139.3.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
80.246.130.172	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
149.78.47.72	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.149	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
85.113.111.134	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
46.121.223.53	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.192.0.20	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
209.126.116.147	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
36.72.228.72	147.237.76.30	Indonesia	himush.idf.il	ET SCAN NMAP -sS window 1024	1
89.133.67.3	147.237.0.35	Hungary	akaws.idf.il	ET SCAN NMAP -sS window 4096	1
80.178.157.115	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.50.77.34	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.139.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.155.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1

03-01-2016 to 03-02-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2756
185.5.223.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1945
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1390
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	512
105.106.139.42	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	426
84.228.172.46	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	278
80.179.114.19	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	212
85.130.231.106	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	210
192.162.26.46	Spain	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	203
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	158
81.218.57.61	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	140
2.54.3.50	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	131
82.102.135.78	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	122
84.108.125.95	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	118
79.178.207.235	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	115
85.130.221.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
69.121.49.39	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
132.64.210.116	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	77
79.180.173.160	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	67
2.102.177.151	United Kingdom	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	66
132.64.210.116	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	55
132.64.210.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	48
89.138.101.168	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
109.65.175.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	48
132.64.210.116	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	46
107.167.107.115	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	44
79.177.149.58	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	44
149.88.215.142	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
109.67.152.165	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
79.176.160.158	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
84.109.6.54	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
79.177.206.134	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	37
176.13.7.209	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.182.132.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	35
84.94.92.164	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
108.39.83.54	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
176.13.11.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	32
178.52.39.29	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	31
178.52.39.29	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	31
46.19.85.244	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
176.13.20.155	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
38.93.232.120	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	30
46.19.85.93	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
83.130.127.221	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
109.253.156.81	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
5.29.213.129	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27

03-01-2016 to 03-02-2016

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
176.13.15.152	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
82.80.160.196	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.13.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	235
82.81.64.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	218
46.19.86.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	188
2.54.27.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	170
109.253.211.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	168
2.54.5.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	149
46.19.86.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	144
46.19.85.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	131
176.13.20.171	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	122
2.52.15.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	111
37.26.147.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
46.19.85.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	101
46.19.85.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	98
46.19.85.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	97
46.19.85.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	96
109.253.147.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	93
109.253.132.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	93
87.68.255.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	92
37.26.146.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	91
185.32.179.14	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	86
2.54.28.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	85
176.13.4.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
109.253.206.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	78
188.116.53.231	Poland	147.237.76.200	eitan.aka.idf.il	Distributed PHP Attempt	Block	76
2.54.135.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	75
188.116.53.231	Poland	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 188.116.53.231	Block	75
46.19.85.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	75
2.54.159.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	73
37.26.149.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	73
46.19.86.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	68
37.26.147.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
109.253.140.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	57
2.52.182.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	57
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	54
109.253.143.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	53
176.13.18.87	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	53
109.160.131.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	52
46.210.242.140	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.210.242.140	Block	52
2.54.27.105	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	51
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	49
109.66.100.184	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	49
46.19.85.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	48
109.253.213.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	46
109.253.129.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
176.13.8.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
2.54.148.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
37.26.148.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	41
109.253.141.185	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 192.115.64.250	Block	37
31.154.94.50	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 31.154.94.50	Block	36

03-01-2016 to 03-02-2016