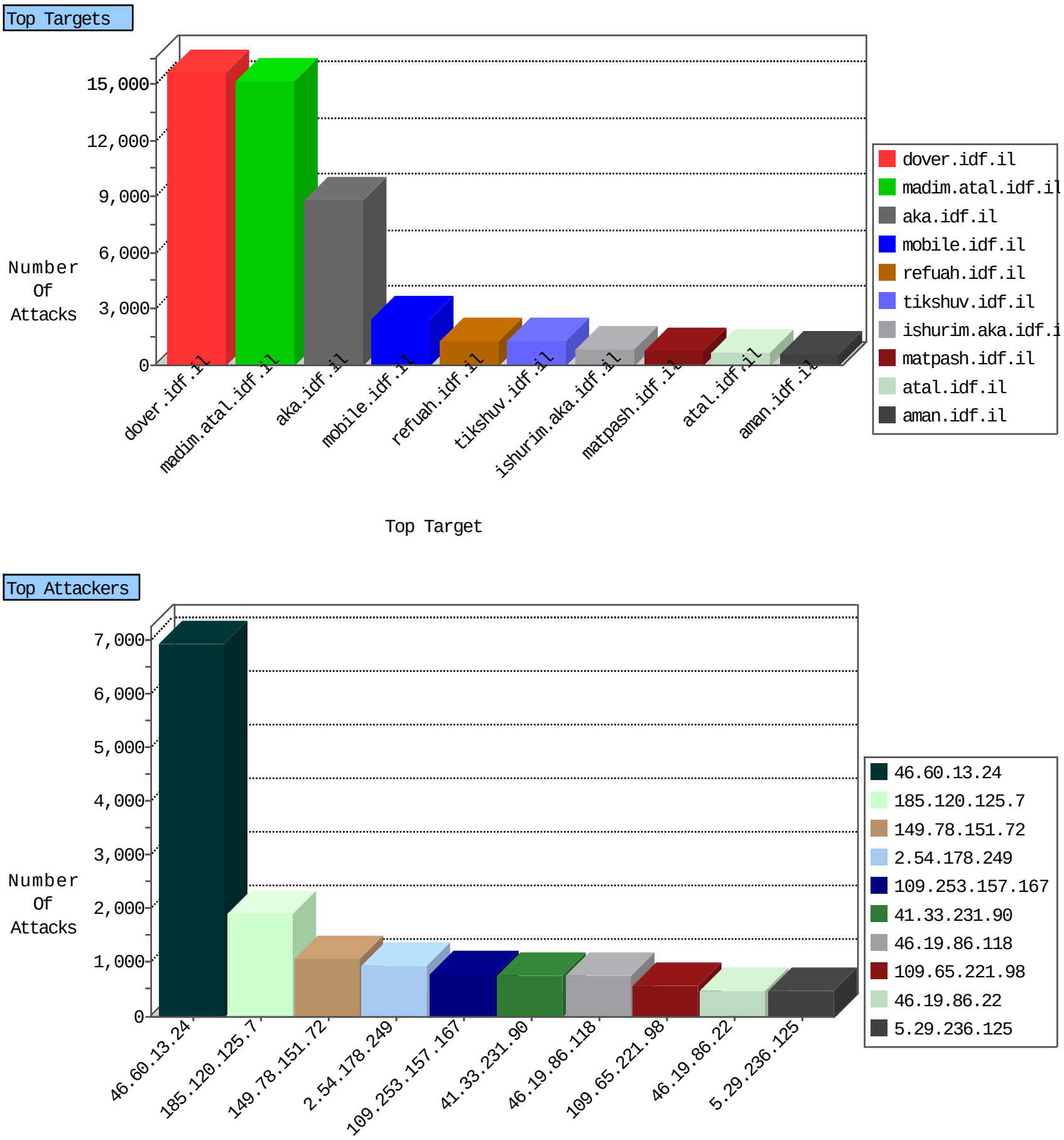
02-01-2016 to 02-02-2016

IDF Under Attack Daily Report



02-01-2016 to 02-02-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.245	Israel	147.237.77.243	mobile.idf.il	TCP handshake violation, first packet not syn	drop	7603
208.109.97.62	United States	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	1817
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	1188
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	811
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	622
109.253.208.118	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	184
121.210.9.93	Australia	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	129
212.199.112.144	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
176.12.155.36	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61
41.43.246.76	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	38
41.43.246.76	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	34
41.43.252.5	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	19
197.36.62.107	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	18
41.43.252.5	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	17
41.239.86.162	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	14
82.132.235.250	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
46.19.85.19	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
41.239.86.162	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	12
197.36.62.107	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	11
41.43.241.123	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	9
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	8
84.109.112.43	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
92.220.58.196	Norway	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
79.180.200.166	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.180.200.166	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
41.43.241.123	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6
37.142.64.102	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
212.179.54.237	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	6
82.145.219.75	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
31.168.19.190	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	5
41.43.194.157	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	5
82.145.216.207	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
41.43.214.245	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	4
37.26.148.181	Israel	147.237.72.166	aka.idf.il	SYN Flood unverified cookie	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
41.47.56.154	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	3
41.43.214.245	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	3
46.19.86.22	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
212.179.64.162	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
31.168.240.21	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.206.82	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
147.236.238.250	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
52.53.253.180	United States	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	3
45.35.64.142		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
79.181.19.95	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
84.108.85.95	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3

02-01-2016 to 02-02-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.45.30.212	Egypt	147.237.77.216	dover.idf.il	C158: HTTP(S): Hacked in the Payload	Block	7
192.116.50.134	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	4
38.87.46.138	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	4
192.116.50.134	Israel	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	4
151.80.31.151	Italy	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	4
151.80.31.150	Italy	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	3
151.80.31.154	Italy	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	2
151.80.31.150	Italy	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	2
151.80.31.151	Italy	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	2
151.80.31.151	Italy	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	2
45.56.148.27		147.237.77.74	law.idf.il	C008: HTTP: Xenu UserAgent	Block	2
212.179.225.88	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	2
52.26.202.58	United States	147.237.77.176	matpash.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
198.50.134.71	Canada	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
77.248.12.153	Netherlands	147.237.76.42	refuah.idf.il	14331: HTTP: Suspicious User-Agent (My Session)	Block	1
46.119.118.213	Ukraine	147.237.76.147	chinuch.aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
188.165.225.121	France	147.237.72.166	aka.idf.il	0543: HTTP: php.cgi Access	Block	1
94.142.39.246	Jordan	147.237.77.74	law.idf.il	C008: HTTP: Xenu UserAgent	Block	1
192.116.50.134	Israel	147.237.76.86	navy.idf.il	C008: HTTP: Xenu UserAgent	Block	1
52.26.202.58	United States	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
151.80.31.154	Italy	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	1
151.80.31.150	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1
81.213.95.118	Turkey	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
212.63.108.252	Spain	147.237.77.74	law.idf.il	0527: HTTP: formmail.pl Access	Block	1
51.254.141.46	United Kingdom	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
188.165.225.121	France	147.237.77.216	dover.idf.il	0543: HTTP: php.cgi Access	Block	1
104.151.242.62	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
192.116.50.134	Israel	147.237.77.170	maarachot.idf.il	C008: HTTP: Xenu UserAgent	Block	1
52.32.210.122	United States	147.237.77.176	matpash.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
151.80.31.154	Italy	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	1
82.123.131.245	France	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1
212.63.108.252	Spain	147.237.77.74	law.idf.il	3885: HTTP: PHP File Include Exploit	Block	1
52.26.202.58	United States	147.237.72.166	aka.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
188.165.225.121	France	147.237.77.216	dover.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
151.80.31.152	Italy	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
52.32.210.122	United States	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
45.56.148.27		147.237.77.176	matpash.idf.il	C008: HTTP: Xenu UserAgent	Block	1
172.86.83.125		147.237.76.86	navy.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
151.80.31.150	Italy	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1
91.121.60.119	France	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
52.26.202.58	United States	147.237.77.74	law.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
191.232.39.241	United States	147.237.77.176	matpash.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
151.80.31.153	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1
5.9.89.170	Germany	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
109.186.169.78	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1
194.181.124.40	Poland	147.237.77.176	matpash.idf.il	C008: HTTP: Xenu UserAgent	Block	1
62.210.97.48	France	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
45.56.148.27		147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
188.165.15.81	France	147.237.77.226	www.chamatz.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-01-2016 to 02-02-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.60.13.24	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	6942
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	61
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	26
109.65.137.228	147.237.77.176	Israel	matpash.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	24
46.19.85.238	147.237.76.42	Israel	refuah.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	22
66.249.65.43	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	22
124.114.151.87	147.237.0.34	China	tikshuv.idf.il	ET WEB_SERVER Possible SQL Injection (varchar)	10
2.54.190.233	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	10
41.45.30.212	147.237.77.216	Egypt	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	9
54.69.65.50	147.237.77.233	United States	atal.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	8
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	5
31.44.135.196	147.237.77.216	Israel	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
66.102.9.6	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
58.221.242.130	147.237.72.156	China	aman.idf.il	GPL SCAN nmap TCP	2
77.127.238.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
62.90.131.234	147.237.77.216	Israel	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
79.180.98.52	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
109.253.201.154	147.237.77.243	Israel	mobile.idf.il	GPL SCAN myscan	2
66.249.93.123	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
95.86.96.216	147.237.72.166	Israel	aka.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	2
212.76.99.155	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
190.196.59.34	147.237.76.177	Chile	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.78.159	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.89	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
37.26.147.211	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
193.105.134.220	147.237.8.14	Sweden	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	2
168.62.238.153	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
115.29.224.200	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
109.253.201.154	147.237.77.243	Israel	mobile.idf.il	INDICATOR-SCAN myscan	2
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
2.54.174.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
195.160.242.40	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
173.55.32.113	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.159	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
112.26.207.25	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.54.157.183	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.138.163.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
207.167.42.153	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.225.55	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.107	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
128.39.168.79	147.237.8.46	Norway	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
36.72.228.72	147.237.76.42	Indonesia	refuah.idf.il	ET SCAN NMAP -sS window 2048	1
105.228.205.242	147.237.76.202	South Africa	e.halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.246.0.97	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
84.94.113.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.72.217	Sweden	e.idf.il	ET SCAN NMAP -sS window 1024	1
84.117.113.152	147.237.77.226	Romania	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1

02-01-2016 to 02-02-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1275
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	720
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	636
169.145.3.40	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	396
178.116.98.100	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	357
79.181.225.55	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	204
212.76.127.219	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	171
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	167
173.208.123.26	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	145
79.178.170.8	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	130
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	104
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	89
141.0.15.61	Europe	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	87
77.126.58.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	80
41.43.246.76	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
80.246.130.59	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	62
109.253.131.127	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	drop	SAM rule	drop	58
46.19.86.151	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	57
46.120.154.62	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	56
41.43.252.5	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
8.37.237.141	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	54
80.246.130.73	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
197.36.62.107	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
37.26.148.197	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	53
213.55.104.210	Ethiopia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
41.239.86.162	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
2.54.146.163	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	50
2.52.13.83	Israel	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	46
85.65.48.121	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
109.67.157.180	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
141.0.14.82	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	38
79.178.177.60	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
31.168.123.247	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
77.127.148.5	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
46.19.85.43	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
2.54.159.215	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
212.179.214.113	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.180.112.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.121.156.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.54.146.163	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	35
80.246.130.188	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
62.0.197.105	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	34
46.19.86.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	34
5.43.199.10	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	34
46.19.85.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
79.176.100.149	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
112.198.103.151	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	31

02-01-2016 to 02-02-2016

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.178.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	671
149.78.151.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	644
46.19.86.118	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.118	Block	503
109.253.157.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	476
109.65.221.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	322
5.29.236.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	307
149.78.151.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	288
46.19.86.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	279
2.54.178.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	264
109.65.221.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	261
176.12.155.0	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	243
109.253.133.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	239
176.12.154.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	187
109.253.157.167	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 109.253.157.167	Block	175
176.12.155.0	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	173
109.253.147.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	171
109.253.147.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	171
2.54.38.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	162
176.12.154.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	161
5.29.236.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	156
46.19.86.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	156
149.78.151.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	146
109.253.203.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	143
109.253.219.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	141
37.26.148.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	138
2.52.38.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	135
109.253.203.240	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.203.240	Block	135
109.253.157.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	133
37.26.147.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	132
176.13.15.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	132
176.12.155.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	131
176.12.154.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	130
46.19.86.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	128
37.26.149.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	127
109.253.133.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	126
37.26.149.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	124
46.19.86.118	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 46.19.86.118	Block	123
176.12.154.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	120
176.12.155.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	119
2.52.165.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	117
46.19.86.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	114
46.19.86.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	113
2.52.165.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	112
2.54.179.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	111
109.253.221.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
46.19.85.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	109
2.54.179.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
2.54.38.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
37.26.148.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
79.176.240.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	102

02-01-2016 to 02-02-2016