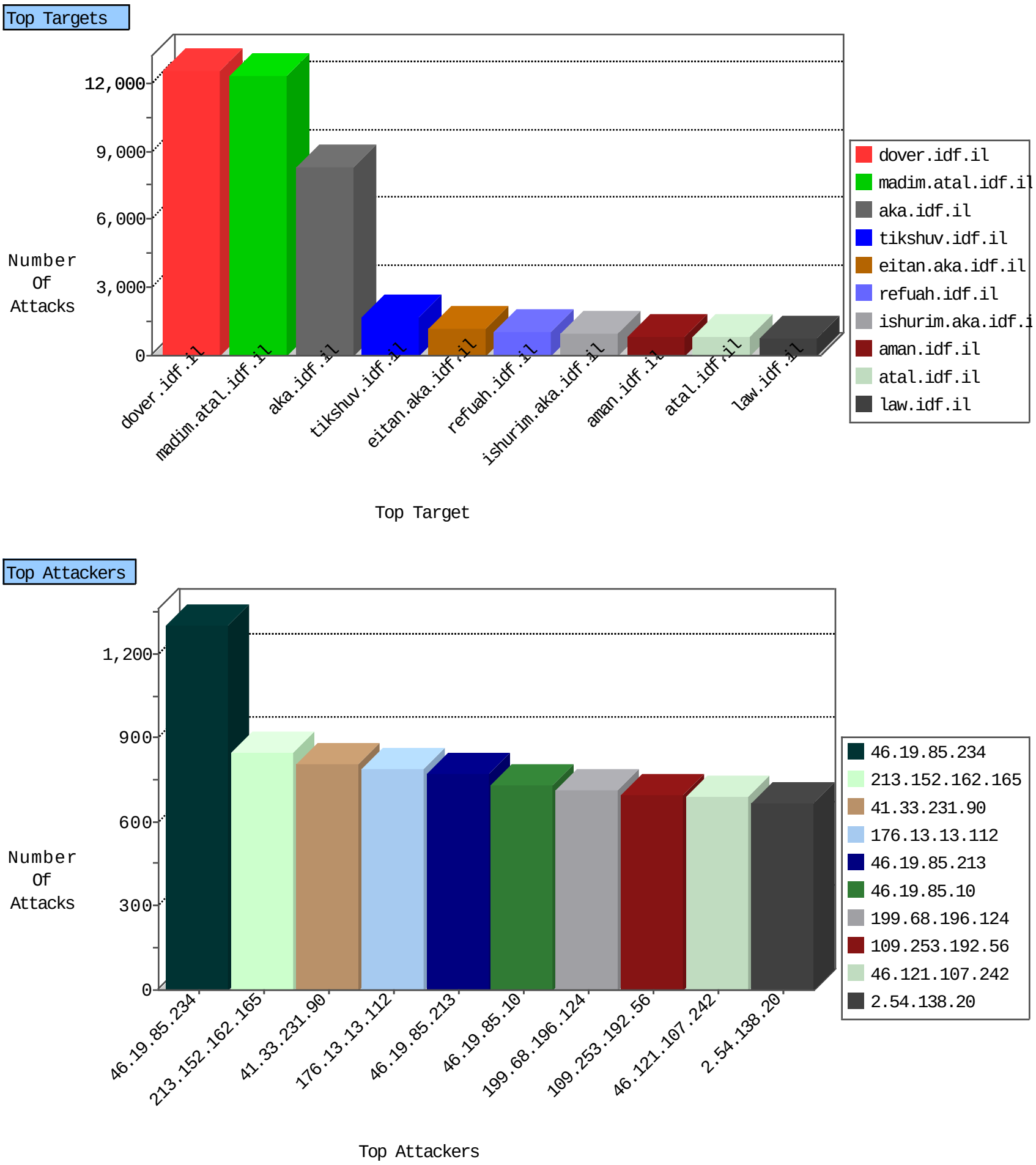
02-21-2016 to 02-22-2016

IDF Under Attack
Daily Report



02-21-2016 to 02-22-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.178.40	Israel	147.237.76.147	chinuch.aka.idf.il	TCP Scan (vertical)	drop	3921
204.93.154.210	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	3715
67.220.158.14	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3381
213.152.162.165	Netherlands	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	3166
66.249.66.33	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3010
185.57.80.147	Romania	147.237.77.216	dover.idf.il	HTTP-MISC-Slow-HTTP-Test-DoS	source-reset	2062
213.152.162.165	Netherlands	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1711
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1458
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	692
199.68.196.124	United States	147.237.77.216	dover.idf.il	DOS-Apache-httpd-apr2-BO	dest-reset	603
37.26.146.163	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	396
207.232.36.181	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	318
89.163.150.79	Germany	147.237.77.216	dover.idf.il	DOS-Apache-httpd-apr2-BO	dest-reset	300
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	253
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	195
204.93.154.198	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	195
178.32.53.94	United Kingdom	147.237.77.216	dover.idf.il	DOS-Apache-httpd-apr2-BO	dest-reset	185
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	153
37.236.188.24	Iraq	147.237.77.216	dover.idf.il	HTTP-MISC-Havij-User-Agent	dest-reset	148
213.152.162.165	Netherlands	147.237.77.216	dover.idf.il	HTTP-MISC-Slow-HTTP-Test-DoS	source-reset	144
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
89.163.150.79	Germany	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	88
195.244.23.42	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	55
109.65.112.60	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	51
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	33
178.32.53.94	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	25
85.65.188.110	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	19
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	18
199.229.243.161	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	17
79.177.161.99	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	12
185.120.125.41		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
89.163.150.79	Germany	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
109.160.147.207	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
178.32.53.94	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	7
79.183.183.239	Israel	147.237.72.156	aman.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
79.183.183.239	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
112.133.248.4	India	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
87.69.106.238	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
46.19.85.186	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
46.19.85.226	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
70.199.77.29	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
2.54.55.230	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
109.64.104.75	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
213.8.204.70	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
115.239.228.10	China	147.237.76.39	mobile.meitav.idf.il	JLM_Under_Attack_Con_Http	drop	4
5.196.80.160	France	147.237.77.233	atal.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	4
77.222.205.193	Norway	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4

02-21-2016 to 02-22-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.88.92.198	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	29
138.134.102.15	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	24
91.228.248.251	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	24
212.25.106.78	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	21
106.120.173.109	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	20
194.114.146.227	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	19
157.55.39.97	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	19
79.182.211.235	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
149.88.3.143	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	13
138.134.102.16	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
62.90.100.26	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
5.29.193.165	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
157.55.39.216	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	9
94.102.153.58	United Kingdom	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	8
46.120.49.242	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
84.228.217.94	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
79.176.99.193	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
84.109.68.240	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
149.88.143.84	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
84.111.29.9	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.183.137.1	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	8
79.180.217.32	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.66.3.182	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
84.111.209.100	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	8
87.71.42.114	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
80.246.130.224	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
80.246.133.111	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
46.19.85.96	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
2.54.177.241	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
157.55.39.97	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
82.166.154.239	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
79.180.241.238	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
84.228.197.36	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
80.246.130.224	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
213.246.56.158	France	147.237.72.156	aman.idf.il	C1000106: HTTP: majestic bot	Block	6
62.219.165.220	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
109.64.110.65	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
185.120.125.2		147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
40.77.167.71	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
5.196.80.160	France	147.237.77.233	atal.idf.il	10767: HTTP: Acunetix Security Scanner	Block	4
109.64.35.112	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
88.160.233.248	France	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	4
184.173.233.226	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
94.102.153.58	United Kingdom	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
85.65.11.200	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
37.205.0.49	Turkey	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
79.179.124.58	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
195.140.210.83	Germany	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4

02-21-2016 to 02-22-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.102.9.101	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	185
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	67
66.249.75.231	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	40
94.102.153.58	147.237.77.216	United Kingdom	dover.idf.il	SQL Injection - Select From	36
2.52.178.40	147.237.76.147	Israel	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	13
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	12
81.218.22.216	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	7
37.205.0.49	147.237.72.166	Turkey	aka.idf.il	SQL Injection - Select From	6
184.173.233.226	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
202.124.109.87	147.237.77.233	New Zealand	atal.idf.il	SQL Injection - Select From	6
95.86.121.217	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
195.140.210.83	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	5
174.37.194.144	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sA (2)	4
2.52.160.0	147.237.76.147	Israel	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	3
82.80.17.163	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	3
2.54.42.108	147.237.72.156	Israel	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	3
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
185.3.144.98	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
109.65.62.59	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
188.120.148.141	147.237.77.216	Israel	dover.idf.il	ET SCAN NMAP -sA (2)	2
87.69.37.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
218.246.0.97	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	2
202.152.254.236	147.237.76.38	Indonesia	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.128	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sA (2)	2
80.246.130.180	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
202.152.254.236	147.237.8.28	Indonesia	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
202.152.254.236	147.237.77.227	Indonesia	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
80.178.13.89	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
202.152.254.236	147.237.76.42	Indonesia	refuah.idf.il	ET SCAN Potential SSH Scan	2
46.19.85.6	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
198.20.69.74	147.237.76.202	United States	e.halag.idf.il	ET DROP Dshield Block Listed Source	2
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
202.152.254.236	147.237.8.45	Indonesia	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
46.117.127.177	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	2
202.152.254.236	147.237.77.176	Indonesia	matpash.idf.il	ET SCAN Potential SSH Scan	2
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
79.182.56.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
177.226.155.227	147.237.76.31	Mexico	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
62.210.7.49	147.237.0.16	France	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.234.38.249	147.237.76.199	Russian Federation	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
37.142.253.88	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.113.125.11	147.237.76.200	Romania	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.213.219.175	147.237.0.33	Romania	idf.il	ET SCAN Potential SSH Scan	1
74.201.85.87	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
125.212.232.146	147.237.76.86	Vietnam	navy.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.204.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.209.141.122	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
5.22.129.99	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.160.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-21-2016 to 02-22-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	784
213.152.162.165	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	610
199.68.196.124	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	603
77.127.207.243	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	465
89.163.150.79	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	306
188.247.77.187	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	173
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	156
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	141
51.255.38.230	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	121
195.189.193.1	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	120
5.22.135.195	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	114
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	99
37.58.52.30	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	93
213.152.162.165	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	93
109.67.55.27	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	87
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	85
94.30.117.177	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	83
178.32.53.94	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	75
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	72
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	69
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	68
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	67
199.68.196.124	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	66
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	65
93.172.28.116	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	62
85.130.238.230	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	59
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	59
109.253.150.70	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
176.13.21.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	55
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	55
185.27.106.99	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
2.52.50.84	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	53
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	52
2.52.22.178	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
87.68.64.205	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
46.121.211.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	50
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	49
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	49
185.57.80.147	Romania	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	49
46.19.85.170	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	48
85.130.245.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
85.130.223.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	47
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	46
109.75.78.25	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	923
46.19.85.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	558
46.19.85.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	551
176.13.13.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	550
46.121.107.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	521
2.54.45.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	499
109.253.192.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	489
46.19.85.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	383
2.54.138.20	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.138.20	Block	376
185.32.179.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	375
46.19.86.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	351
37.26.149.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	344
185.27.105.136	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 185.27.105.136	Block	308
46.19.85.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	245
2.54.138.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	245
176.13.13.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	238
46.19.85.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	211
109.253.192.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	209
84.109.50.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	203
46.19.85.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	180
185.32.179.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	170
81.218.124.66	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 81.218.124.66	Block	169
77.125.5.69	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	168
46.121.107.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	168
109.253.138.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	167
46.19.86.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	139
37.26.149.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	137
176.13.17.122	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.17.122	Block	133
185.27.105.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	133
84.109.50.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	131
109.253.208.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	127
185.32.179.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	124
192.116.255.106	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 192.116.255.106	Block	120
176.13.17.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	118
46.19.85.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	109
79.181.34.234	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.181.34.234	Block	107
176.13.17.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
82.102.169.113	Israel	147.237.76.39	mobile.meitav.idf.il	Distributed Suspicious Response Code	Block	104
185.32.179.199	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 185.32.179.199	Block	102
176.13.18.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
176.13.17.169	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.17.169	Block	89
37.26.148.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
109.253.150.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
46.19.85.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
5.28.161.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
46.117.25.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	73
109.253.208.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	72
82.102.169.113	Israel	147.237.76.39	mobile.meitav.idf.il	Too Many of the Same Response Code (400) in Session from 82.102.169.113	Block	72
2.54.161.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	72
82.80.192.100	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many of the Same Response Code (404) in Session from 82.80.192.100	Block	70