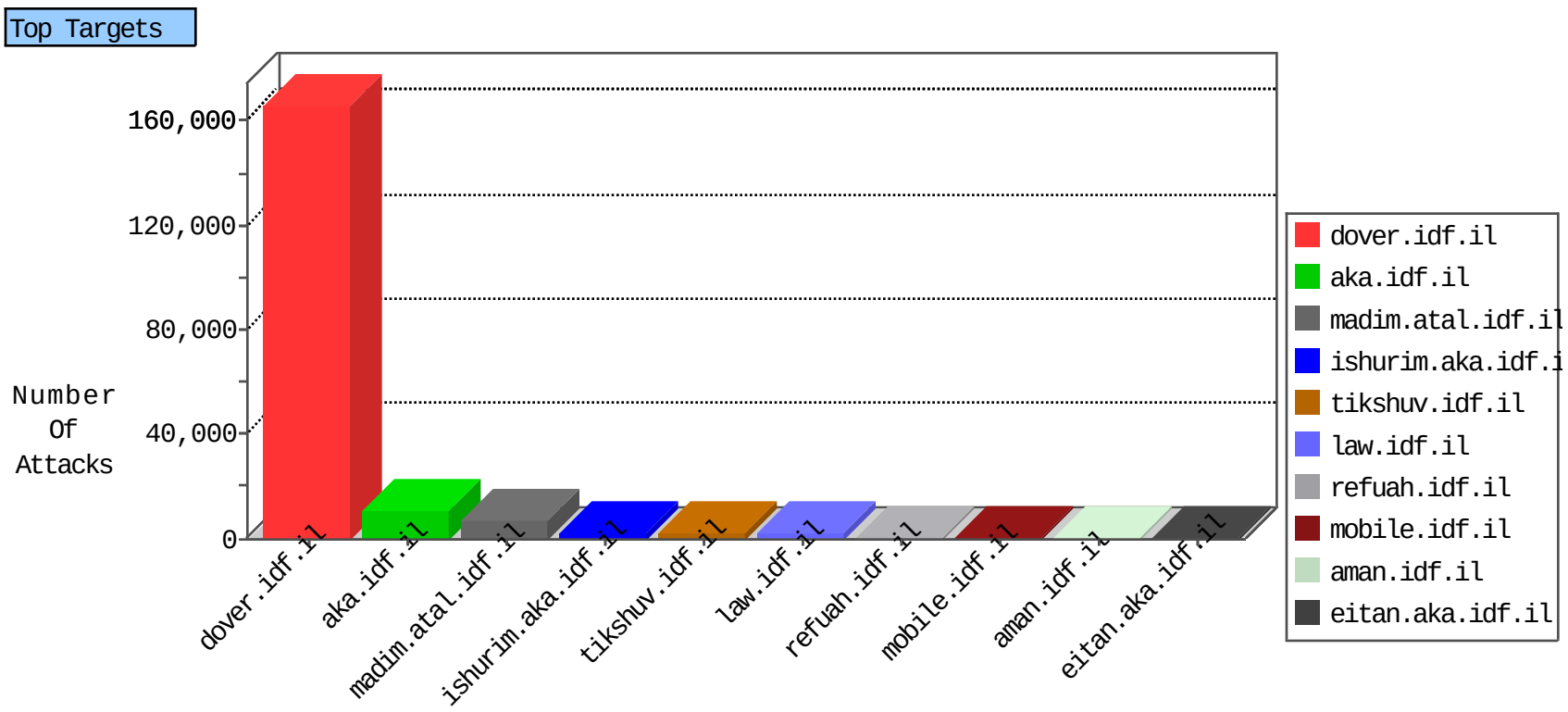
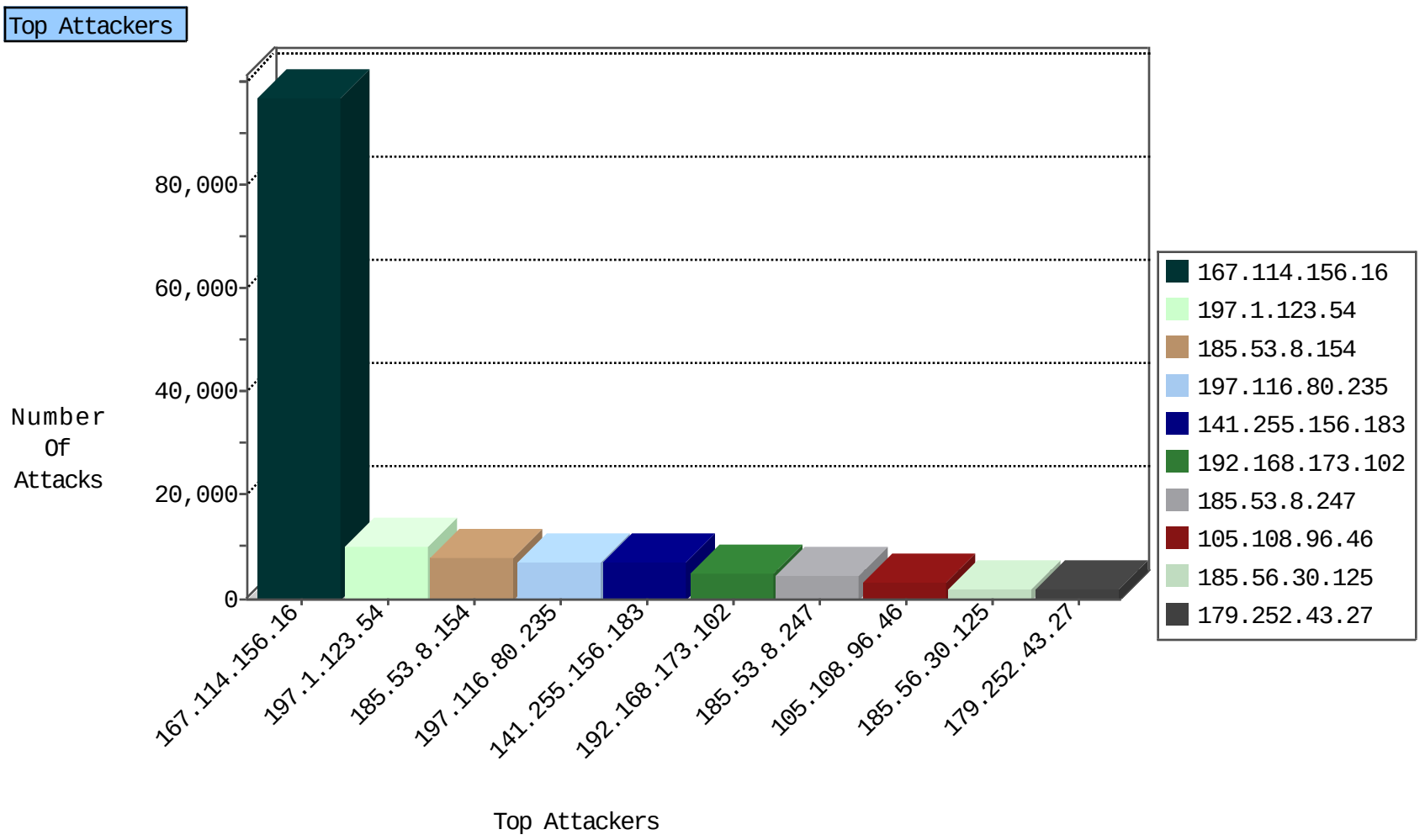
04-11-2016 to 04-12-2016

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-11-2016 to 04-12-2016

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	Block_Ip_Web_In	drop	97192
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	34361
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	33898
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	20358
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5173
179.252.43.27	Brazil	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	3888
179.252.43.27	Brazil	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	3717
83.130.99.162	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1917
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1850
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1373
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1305
41.111.97.43	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1087
109.67.111.179	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	994
176.126.252.11	Romania	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	707
74.206.99.126	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	677
46.117.43.97	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	644
31.210.187.120	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	641
109.253.224.2	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	625
105.107.27.194	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	553
46.244.157.134	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	514
46.19.85.203	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	513
94.159.151.206	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	506
5.28.191.233	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	473
185.3.144.24	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	432
207.232.36.85	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	411
79.168.49.63	Portugal	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	406
83.130.116.167	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	355
80.246.136.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	328
80.178.189.105	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	325
77.158.88.42	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	320
79.181.16.95	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	310
192.243.55.131	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	299
37.26.147.216	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	283
192.243.55.135	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	280
79.180.9.222	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	280
149.56.14.68	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	257
94.230.86.80	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	250
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	250
2.53.52.79	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	217
80.178.157.42	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	183
197.2.106.182	Tunisia	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	155
77.158.89.41	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	150
77.125.160.127	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	149
156.203.75.175	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	142
87.70.88.156	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	136
62.219.140.244	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	134
197.2.106.182	Tunisia	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	133
94.159.130.204	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	131
192.243.55.137	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	128
192.243.55.136	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	121

04-11-2016 to 04-12-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.150	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	42
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	25
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	24
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	23
61.135.189.99	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	21
106.120.173.85	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	21
213.8.204.2	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	17
84.94.180.40	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
82.81.14.26	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
109.253.134.127	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
109.65.20.19	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
212.143.110.33	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
77.125.95.194	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
79.178.26.28	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
79.179.22.91	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
37.26.148.237	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
84.108.93.19	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
91.197.103.1	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
109.253.145.79	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
79.179.54.35	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
80.246.130.105	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
109.66.56.208	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
5.28.173.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
46.121.232.50	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
89.139.61.114	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
213.57.188.138	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.19.86.241	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.65.59.235	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
82.102.168.106	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.65.132.84	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
213.8.204.40	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	6
46.19.86.158	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
80.91.162.99	Ukraine	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	6
149.88.229.120	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
109.67.111.179	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
79.182.173.139	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
82.81.76.144	Israel	147.237.77.170	maarachot.idf.il	C1000008: HTTP: Xenu UserAgent	Block	6
62.90.88.104	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
88.198.230.79	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	5
80.91.162.99	Ukraine	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	5
213.151.51.210	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
79.176.13.226	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
149.88.47.121	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
79.181.201.140	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
89.138.38.3	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
31.154.31.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
69.30.198.178	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4

04-11-2016 to 04-12-2016

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	67
66.249.93.13	147.237.77.226	Europe	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	48
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	13
94.123.200.108	147.237.77.216	Turkey	dover.idf.il	SERVER-WEBAPP login.htm access	8
94.123.200.108	147.237.77.216	Turkey	dover.idf.il	SERVER-WEBAPP admin.php access	8
106.187.37.163	147.237.77.216	Japan	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	8
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	7
36.79.8.174	147.237.77.170	Indonesia	maarachot.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
37.26.147.153	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	6
36.79.8.174	147.237.77.74	Indonesia	law.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
66.249.64.50	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	5
80.246.139.171	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	4
80.82.78.38	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	4
66.249.78.96	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	3
208.80.155.215	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	3
175.43.95.77	147.237.77.216	China	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	3
132.74.95.19	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
212.106.92.100	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
192.243.55.136	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	2
163.172.140.23	147.237.77.243	United Kingdom	mobile.idf.il	ET SCAN NMAP -sS window 1024	2
5.8.45.2	147.237.77.216	Brazil	dover.idf.il	SQL Injection - Select From	2
66.249.66.56	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
95.235.11.21	147.237.77.216	Italy	dover.idf.il	GPL SCAN nmap TCP	2
174.37.194.144	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sA (2)	2
174.37.194.144	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sA (2)	2
46.116.3.52	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
103.227.20.58	147.237.77.216	Australia	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
185.110.109.190	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	2
192.243.55.135	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	2
208.100.26.228	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
85.65.202.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
174.37.194.144	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
174.37.194.144	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sA (2)	2
89.248.172.140	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
212.150.214.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
188.213.219.175	147.237.0.33	Romania	idf.il	ET SCAN Potential SSH Scan	1
46.19.86.240	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
163.172.140.23	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.53.10.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
107.158.255.194	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
84.109.1.189	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.76.198	United States	e.yohalan.idf.il	ET DROP Dshield Block Listed Source	1
66.249.93.142	147.237.77.74	Europe	law.idf.il	ET SCAN NMAP -sA (2)	1
179.252.43.27	147.237.77.216	Brazil	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.103.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
112.112.56.65	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
37.46.39.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.22.249	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1

04-11-2016 to 04-12-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.53.8.154	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7947
141.255.156.183	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6903
197.1.123.54	Tunisia	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6271
185.53.8.247	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4371
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	3497
105.108.96.46	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2911
197.1.123.54	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2617
185.56.30.125	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1916
204.93.58.84	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	1708
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	1706
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1440
178.220.105.38		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1179
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	750
109.93.54.252		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	747
185.53.8.244	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	738
185.53.8.245	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	716
151.16.41.18	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	581
121.54.44.89	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	537
177.23.207.221	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	464
79.215.228.169	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	402
87.151.231.53	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	335
148.0.182.157	Dominican Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	306
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	drop		drop	264
197.116.80.235	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	243
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	243
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	240
121.54.44.93	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	227
105.108.96.46	Algeria	147.237.77.216	dover.idf.il	drop		drop	171
94.123.200.108	Turkey	147.237.77.216	dover.idf.il	drop	SAM rule	drop	140
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	136
179.252.43.27	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	117
81.218.99.36	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	111
46.19.85.122	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	111
176.13.18.33	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
79.183.70.79	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	105
185.3.146.223	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	90
197.2.106.182	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	87
31.168.230.226	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
192.243.55.133	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	82
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	82
37.26.146.230	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	80
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
31.168.230.226	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	75
171.5.223.153	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
31.168.26.98	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
212.25.86.242	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
192.243.55.129	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	71
192.243.55.132	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	70

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.1.123.54	Tunisia	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	384
197.1.123.54	Tunisia	147.237.77.216	dover.idf.il	Multiple Malformed URL from 197.1.123.54	Block	383
197.1.123.54	Tunisia	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 197.1.123.54	Block	383
2.53.24.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	330
37.26.147.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	287
85.65.230.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	247
185.120.126.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	241
79.177.9.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	232
46.19.85.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	227
95.35.74.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	224
176.13.22.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	221
94.123.200.108	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 94.123.200.108	Block	219
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	218
46.19.85.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	208
46.19.86.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	207
94.123.200.108	Turkey	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 94.123.200.108	Block	205
37.26.149.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	205
46.19.86.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	179
2.54.149.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	176
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 41.107.60.144	Block	170
46.19.85.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	162
185.120.125.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	148
62.219.228.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	148
109.253.210.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	148
80.246.139.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	129
94.123.200.108	Turkey	147.237.77.216	dover.idf.il	PHP Attempt	Block	121
2.55.16.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	120
2.54.191.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
109.253.211.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
46.19.85.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
2.52.129.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
109.253.220.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
109.253.213.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
176.13.1.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
87.69.207.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	101
36.251.131.206	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 36.251.131.206	Block	99
176.13.21.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	95
46.19.85.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	91
176.13.10.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	89
95.35.24.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
109.67.35.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
109.253.221.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
109.253.130.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
37.26.147.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
2.52.166.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	72
2.53.40.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
46.19.85.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
95.35.206.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61

04-11-2016 to 04-12-2016