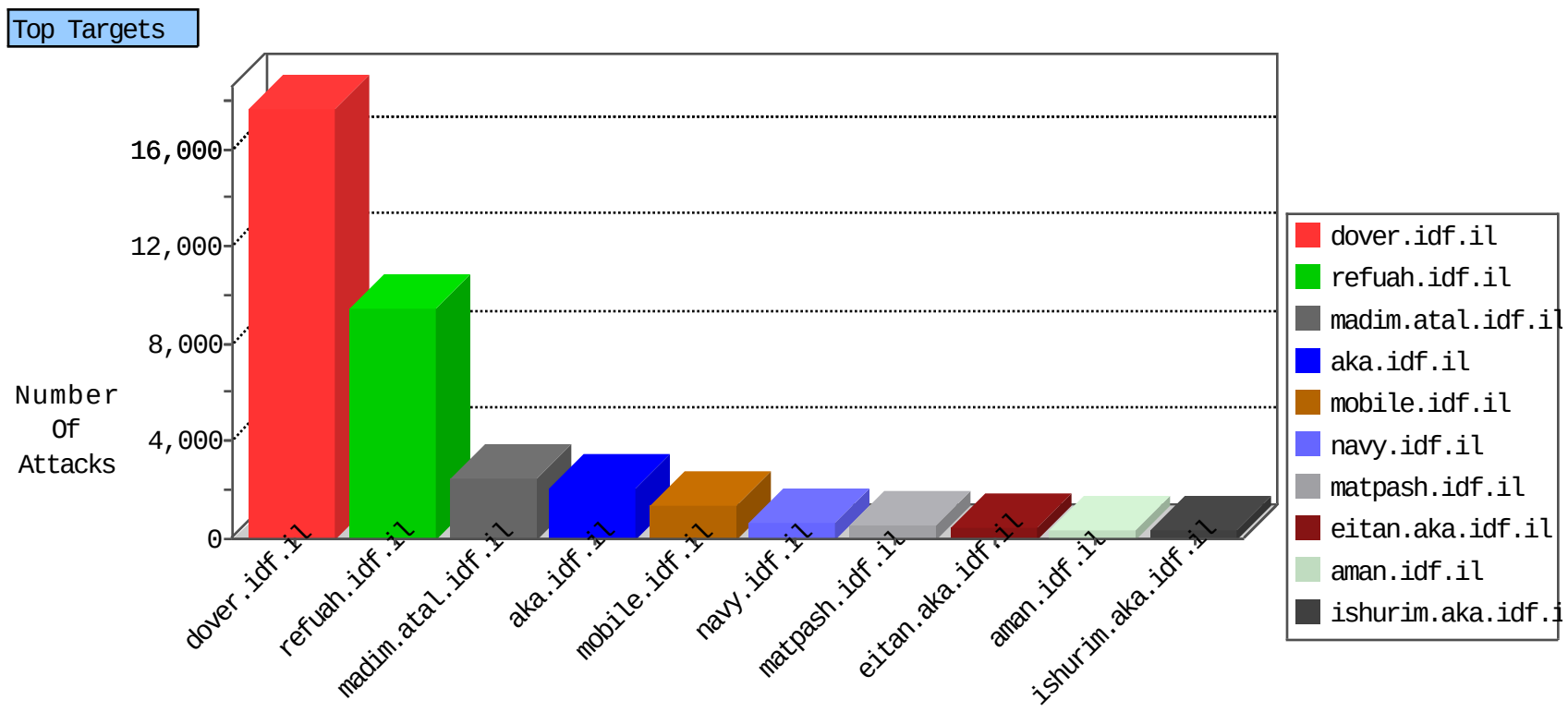
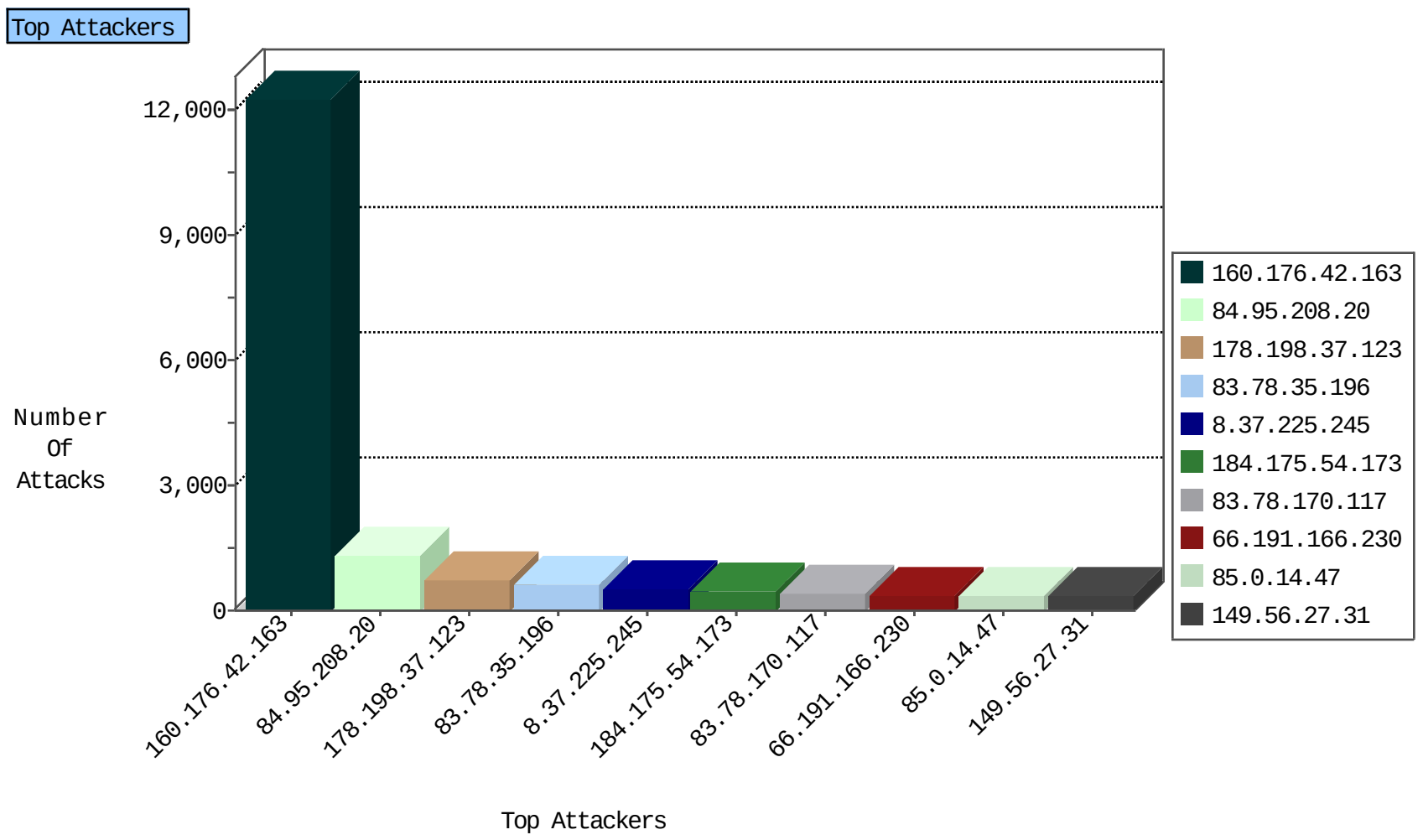
10-02-2016 to 10-03-2016

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-02-2016 to 10-03-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
160.176.42.163	Morocco	147.237.77.216	dover.idf.il	DOS-HTTP-torshammer	dest-reset	245
8.37.225.245	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	80
8.37.225.245	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	59
109.253.192.211	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	52
160.176.42.163	Morocco	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	30
82.145.211.186	Europe	147.237.76.42	refuah.idf.il	Black List	drop	20
82.145.219.189	Europe	147.237.76.86	navy.idf.il	Black List	drop	17
2.55.15.250	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	16
109.253.138.116	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
2.53.45.202	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
46.19.86.233	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
46.121.238.128	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
134.147.203.115	Germany	147.237.76.31	nakchal.idf.il	Black List	drop	6
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
109.67.123.183	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	5
134.147.203.115	Germany	147.237.76.176	test.ncore.idf.il	Black List	drop	5
46.19.85.3	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
8.37.231.238	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	5
66.249.65.52	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
134.147.203.115	Germany	147.237.76.30	himush.idf.il	Black List	drop	3
194.177.16.3	Israel	147.237.76.86	navy.idf.il	Black List	drop	3
8.37.225.245	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
63.141.231.211	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
192.187.101.235	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
198.204.247.221	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
134.147.203.115	Germany	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	2
69.30.226.222	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
134.147.203.115	Germany	147.237.76.201	e.atal.idf.il	Black List	drop	2
192.187.109.58	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
69.30.226.221	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
192.187.118.18	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
192.187.101.234	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
173.208.198.10	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
183.129.255.34	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Http	drop	2
198.204.247.219	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
63.141.242.198	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
134.147.203.115	Germany	147.237.76.202	e.halag.idf.il	Black List	drop	2
69.30.226.221	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
198.204.255.76	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
185.94.111.1	Russian Federation	147.237.76.39	mobile.meitav.idf.il	Black List	drop	2
134.147.203.115	Germany	147.237.76.177	ncore.idf.il	Black List	drop	2
192.187.118.20	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
93.174.94.235	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	2
192.187.101.235	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
198.204.247.220	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
192.187.118.68	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
93.174.94.235	Netherlands	147.237.76.199	e.nakchal.idf.il	Black List	drop	2
63.141.231.213	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
134.147.203.115	Germany	147.237.76.39	mobile.meitav.idf.il	Black List	drop	2

10-02-2016 to 10-03-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.247.14	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	115
69.30.211.2	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	58
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	58
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	32
220.181.125.23	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	25
85.14.244.98	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	11
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	10
193.111.140.106	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	9
85.14.244.113	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	7
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	6
106.38.241.106	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	6
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	6
85.14.244.98	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	5
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	5
162.210.196.130	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	5
193.111.140.106	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	5
162.210.196.97	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	4
162.210.196.129	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
69.30.211.2	United States	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	4
62.210.247.14	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
85.14.244.113	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
91.121.86.136	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
69.30.211.2	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	3
109.90.210.70	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.212.73.211	Netherlands	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
46.4.32.75	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
62.212.73.211	Netherlands	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.213.202	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.210.143.245	France	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
91.121.86.136	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
193.111.140.106	Germany	147.237.77.226	www.chamatz.aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
108.59.8.80	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
5.9.88.103	Germany	147.237.77.226	www.chamatz.aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.106	China	147.237.0.34	tikshuv.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
85.14.244.113	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	1
193.111.140.106	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	1
123.125.125.81	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
85.14.244.98	Germany	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	1
208.51.63.37	United States	147.237.77.216	dover.idf.il	22611: HTTP: WordPress LoginWall Fake Plugin Usage	Block	1
151.80.31.184	France	147.237.77.176	matpash.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
71.6.146.185	United States	147.237.76.39	mobile.meitav.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
151.80.124.186	France	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Permit	1
82.193.127.15	Ukraine	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1
151.80.124.186	France	147.237.77.216	dover.idf.il	C1000018: HTTP: access to administrator/index.php -> Quarantine	Permit	1
85.14.244.113	Germany	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	1

10-02-2016 to 10-03-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.69.112	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	41
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	31
66.249.66.103	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	10
91.121.29.140	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	8
146.200.148.0	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	7
91.121.135.78	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	5
79.180.43.40	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	4
58.218.200.137	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	4
180.66.11.10	147.237.77.234	Korea, Republic of	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	3
208.100.26.228	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	3
58.218.200.137	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	3
66.249.65.51	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	3
5.255.90.133	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	3
190.214.49.3	147.237.8.46	Ecuador	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
58.218.200.137	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
91.224.161.69	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
112.66.17.222	147.237.76.86	China	navy.idf.il	LOCAL_RULES - Request with the string install.php in it	2
154.16.199.48	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	2
62.210.113.73	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
208.100.26.228	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
146.200.148.0	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	2
80.246.130.70	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
59.46.193.114	147.237.8.28	China	e.mobile-ks.idf.il	GPL SCAN nmap TCP	2
192.198.151.44	147.237.72.167	Europe	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
125.65.82.44	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	2
58.218.200.137	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	2
94.102.48.194	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.76.108	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
62.210.113.183	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
183.60.48.25	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
171.247.244.142	147.237.77.216	Vietnam	dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
58.218.200.137	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
91.201.236.158	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	2
218.24.171.223	147.237.8.28	China	e.mobile-ks.idf.il	GPL SCAN nmap TCP	2
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	2
208.100.26.228	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	2
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
46.19.85.48	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
125.65.82.44	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
95.59.136.118	147.237.72.156	Kazakstan	aman.idf.il	ET WEB_SERVER Poison Null Byte	1
218.87.109.253	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
79.177.141.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.40.4.208	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
52.187.42.85	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.72.217	United Kingdom	e.idf.il	ET SCAN NMAP -sS window 1024	1
14.152.59.11	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
114.80.116.202	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.72.156	Ukraine	aman.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
208.100.26.228	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.243.100	147.237.77.170	France	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1

10-02-2016 to 10-03-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
160.176.42.163	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9643
160.176.42.163	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	987
160.176.42.163	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	667
184.175.54.173	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	443
160.176.42.163	Morocco	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	399
8.37.225.245	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	393
66.191.166.230	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	346
92.222.245.134	France	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	257
160.176.42.163	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	233
172.245.202.53	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	203
149.56.27.31	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	202
37.230.210.43	Russian Federation	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	183
98.142.92.46	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	181
83.222.97.147	Russian Federation	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	165
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	159
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	157
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	144
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	137
213.6.74.190	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	136
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	133
83.78.35.196	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	128
83.78.35.196	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	127
160.176.42.163	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	123
83.78.35.196	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	121
2.53.189.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	120
83.78.35.196	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	119
207.46.13.34	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	114
83.78.35.196	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	105
5.22.134.99	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	102
92.241.41.67	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	99
149.56.27.31	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	96
74.91.23.166	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	95
8.37.231.238	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	92
160.176.42.163	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	90
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	87
84.111.14.141	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
83.78.170.117	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	83
83.78.170.117	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	82
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
8.37.225.245	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	79
78.181.92.11	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
85.0.14.47	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	79
85.0.14.47	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	78
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	77
85.0.14.47	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	75
83.78.170.117	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	75
83.78.170.117	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	74
85.0.14.47	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	73
52.3.127.144	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	73

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	734
176.13.246.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	305
213.57.173.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	287
37.26.149.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	247
46.19.85.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	183
77.127.44.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	151
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	143
109.65.125.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	134
37.26.147.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	133
89.139.112.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	114
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	110
5.29.131.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
141.226.218.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
2.55.53.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
2.53.182.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
79.179.10.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	44
95.35.158.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
109.253.132.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	38
80.246.138.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
185.32.179.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	29
109.253.206.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	28
212.76.119.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
109.64.175.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	25
79.178.227.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
176.13.20.144	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 176.13.20.144	Block	23
120.86.186.204	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 120.86.186.204	Block	19
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	18
14.127.67.88	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 14.127.67.88	Block	17
14.127.67.88	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 14.127.67.88	Block	16
120.86.186.204	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 120.86.186.204	Block	15
2.53.61.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	14
37.46.39.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	12
79.178.13.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
109.253.219.102	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	10
77.138.139.237	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.139.237	Block	8
120.86.186.204	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	7
5.28.146.103	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	7
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	7
198.200.98.199	Canada	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	7
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.52	Block	7
31.154.45.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
14.127.67.88	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	6
120.86.186.204	China	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	6