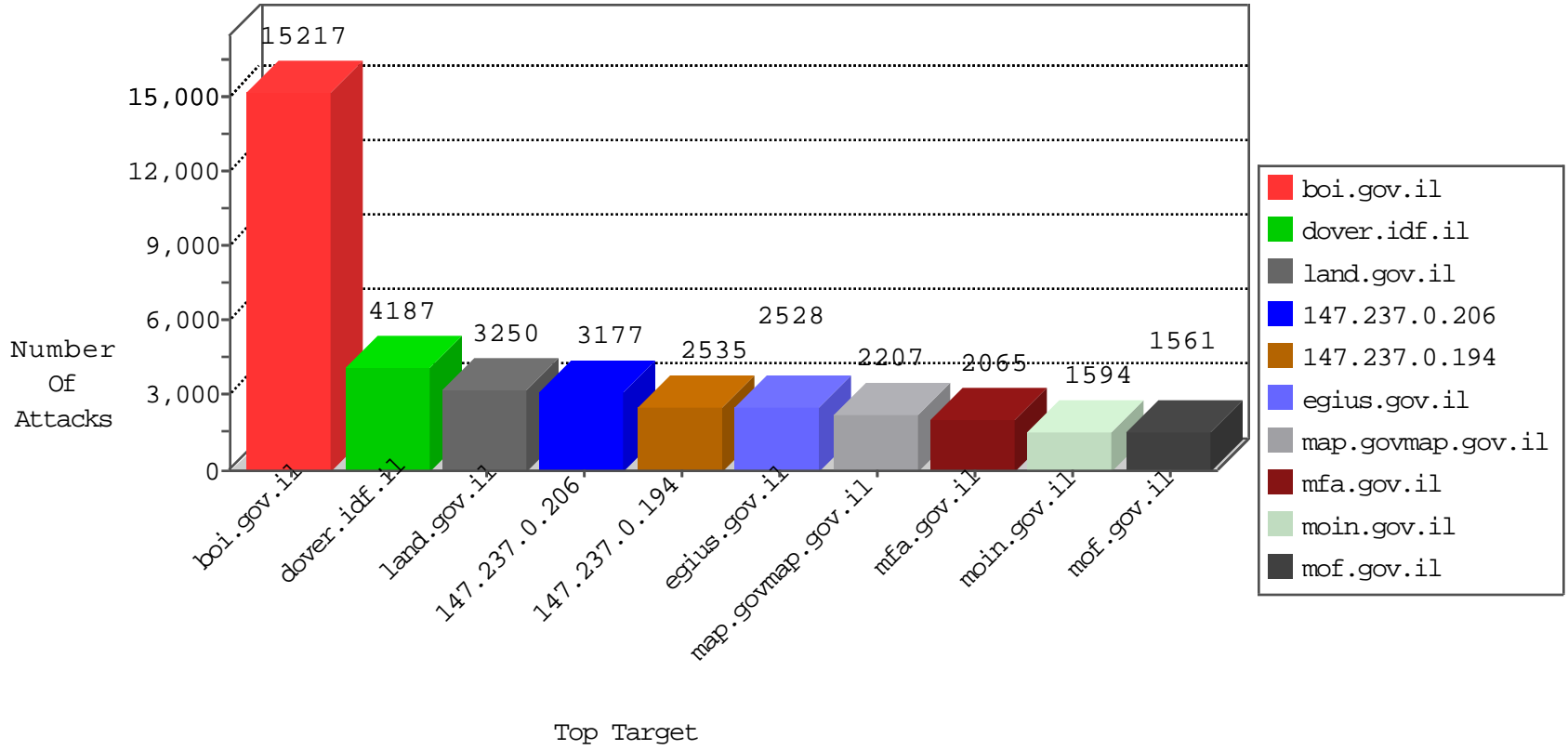




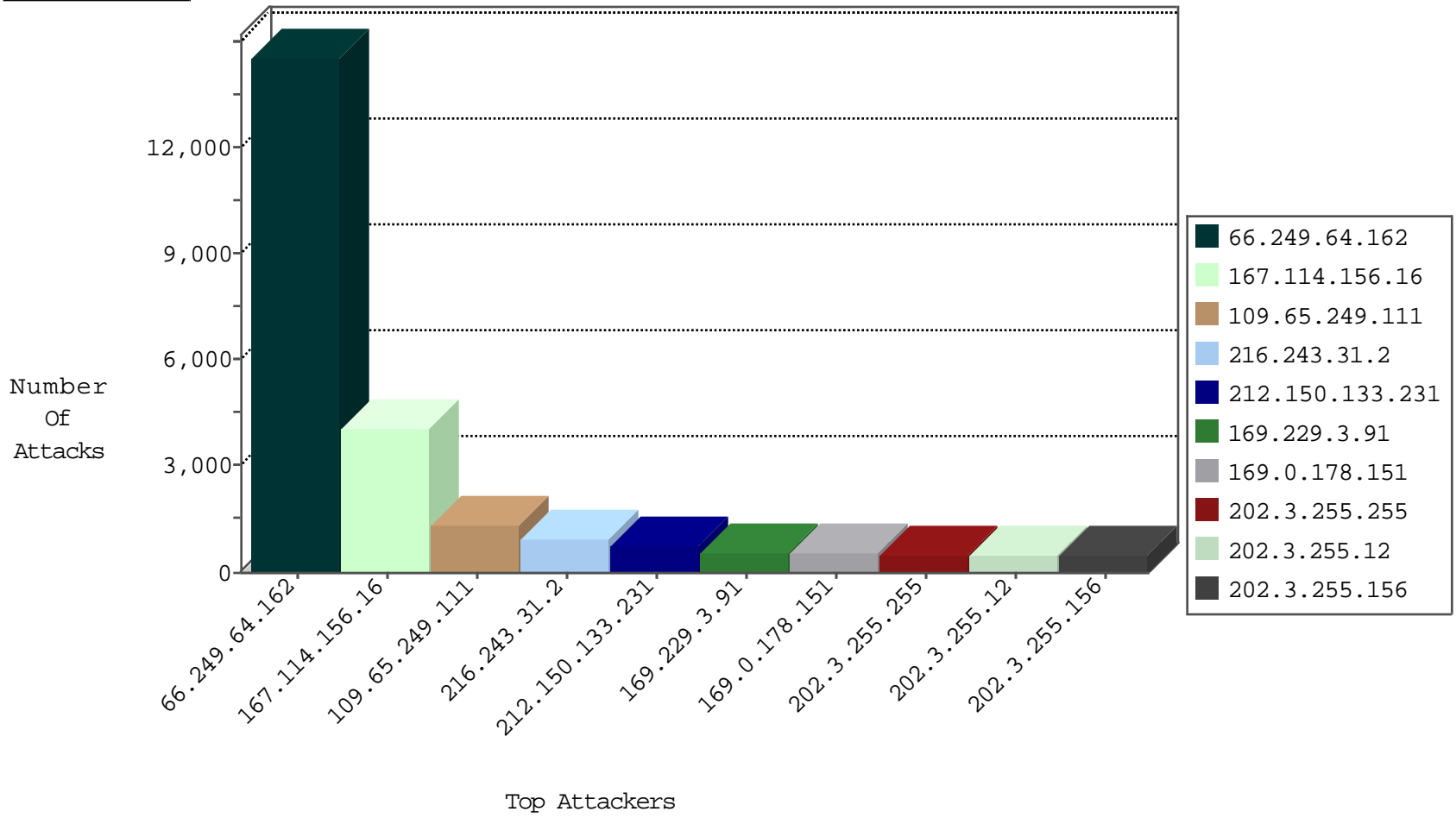
Tehila Hosting Under Attack



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Signature	Device Action
0.0.0.0	147.237.0.206		drop	83
0.0.0.0	147.237.72.77		drop	4
0.0.0.0	147.237.76.106		drop	5
0.0.0.0	147.237.76.106		forward	63
0.0.0.0	147.237.76.155		drop	2
0.0.0.0	147.237.77.216		drop	2
2.55.0.136	147.237.0.206	Israel	drop	2
2.55.141.74	147.237.77.77	Israel	dest-reset	1
5.1.80.100	147.237.1.5	Germany	drop	4
5.1.80.100	147.237.2.5	Germany	drop	2
5.1.80.100	147.237.3.5	Germany	drop	1
5.1.80.100	147.237.77.80	Germany	drop	2
5.9.89.170	147.237.76.106	Germany	forward	8
5.22.129.71	147.237.0.206	Israel	drop	1
5.22.129.251	147.237.0.206	Israel	drop	4
5.22.135.190	147.237.0.206	Israel	drop	11
5.22.135.214	147.237.72.77	Israel	drop	8
5.29.189.74	147.237.0.206	Israel	drop	4
5.29.193.19	147.237.76.157	Israel	drop	3
5.102.195.115	147.237.0.206	Israel	drop	2
5.102.232.31	147.237.0.206	Israel	drop	3
5.102.242.16	147.237.0.206	Israel	drop	91
5.102.243.186	147.237.0.206	Israel	drop	3
5.102.254.4	147.237.0.206	Israel	drop	2
5.102.254.142	147.237.0.206	Israel	drop	10
5.245.158.68	147.237.76.106	Saudi Arabia	forward	2
5.245.158.68	147.237.76.106	Saudi Arabia	forward	2
8.37.224.190	147.237.76.106	United States	forward	10
8.37.224.190	147.237.76.106	United States	forward	10
8.37.225.72	147.237.76.106	United States	drop	2
8.37.225.74	147.237.76.106	United States	drop	2
10.0.0.1	147.237.0.206		drop	6
14.147.0.147	147.237.6.157	China	drop	1
14.185.67.15	147.237.14.60	Vietnam	drop	12
23.94.103.201	147.237.1.107	United States	forward	9
23.94.103.201	147.237.1.107	United States	forward	8
31.14.135.229	147.237.0.227	Romania	drop	1
31.186.250.60	147.237.14.250	Germany	drop	2
31.210.186.132	147.237.0.206	Israel	drop	1
31.210.187.100	147.237.0.206	Israel	drop	1
31.210.187.101	147.237.0.206	Israel	drop	12
31.210.187.117	147.237.0.206	Israel	drop	34
31.210.188.95	147.237.0.206	Israel	drop	1
37.46.38.72	147.237.0.206	Israel	drop	1
37.46.41.60	147.237.0.206	Israel	drop	1
37.142.64.31	147.237.76.26	Israel	drop	3
37.142.226.38	147.237.0.206	Israel	drop	1
40.77.167.53	147.237.72.38	United States	drop	1
41.108.148.101	147.237.76.106	Algeria	forward	114
41.108.148.101	147.237.76.106	Algeria	forward	114

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Name	Device Action	Count
31.168.245.179	147.237.0.49	Israel	16471: HTTP: TeamViewer Communication Attempt	Block	213
5.9.59.79	147.237.72.42	Germany	19863: HTTP: WordPress Revslider/Showbiz PHP File Upload	Block	11
92.63.106.216	147.237.77.225	Russian Federation	14459: HTTP: Known Skunkx DDOS Bot User-Agent Cyberdog	Block	2
84.94.200.163	147.237.77.199	Israel	3624: HTTP: SQL Injection (SELECT)	Block	2
92.63.106.216	147.237.77.225	Russian Federation	16063: HTTP: Suspicious User-Agent (Opera/8.xx) Likely Win32/Ranbyus	Block	2
79.183.129.192	147.237.77.77	Israel	15323: HTTP: User-Agent (MRSPUTNIK)	Block	1
142.54.167.98	147.237.72.134	United States	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
185.120.126.8	147.237.77.130	Israel	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	1
196.184.32.220	147.237.0.71	Tunisia	10725: TCP: LOIC DDoS Tool	Block	1
66.249.66.47	147.237.76.172	Israel	3886: HTTP: Cross Site Scripting in POST Request	Block	1
79.183.129.192	147.237.72.103	Israel	15323: HTTP: User-Agent (MRSPUTNIK)	Block	1
142.54.167.98	147.237.77.104	United States	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
192.115.83.5	147.237.77.199	Israel	3624: HTTP: SQL Injection (SELECT)	Block	1
197.45.65.198	147.237.77.216	Egypt	5141: HTTP: Sqlmap HTTP Request	Block	1
39.57.53.191	147.237.72.201	Pakistan	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Name
2.53.2.248	147.237.0.64	Israel	1
2.53.6.78	147.237.76.192	Israel	2
2.53.26.54	147.237.76.136	Israel	1
2.53.36.93	147.237.0.64	Israel	2
2.53.39.140	147.237.0.64	Israel	1
2.53.60.74	147.237.0.64	Israel	1
2.53.133.51	147.237.76.136	Israel	4
2.53.133.86	147.237.0.64	Israel	4
2.53.148.14	147.237.76.136	Israel	1
2.53.148.239	147.237.76.136	Israel	1
2.53.167.83	147.237.76.26	Israel	8
2.53.174.200	147.237.77.238	Israel	5
2.53.184.19	147.237.0.64	Israel	2
2.55.16.167	147.237.0.64	Israel	1
2.55.62.224	147.237.0.64	Israel	2
2.55.190.178	147.237.76.51	Israel	2
2.134.165.100	147.237.77.225	Kazakstan	4
2.216.192.89	147.237.77.18	United Kingdom	2
5.9.59.79	147.237.72.42	Germany	7
5.18.104.55	147.237.77.225	Russian Federation	3
5.22.130.118	147.237.76.26	Israel	1
5.22.131.57	147.237.0.64	Israel	1
5.22.131.89	147.237.0.64	Israel	15
5.22.135.118	147.237.77.209	Israel	1
5.28.135.19	147.237.77.18	Israel	1
5.28.144.81	147.237.0.64	Israel	2
5.28.184.245	147.237.0.64	Israel	2
5.28.187.147	147.237.77.130	Israel	1
5.29.1.126	147.237.76.26	Israel	1
5.29.17.211	147.237.76.26	Israel	3
5.29.62.144	147.237.0.64	Israel	2
5.29.95.137	147.237.0.64	Israel	1
5.29.181.155	147.237.76.26	Israel	14
5.29.230.7	147.237.0.64	Israel	1
5.29.238.214	147.237.76.134	Israel	2
5.29.241.16	147.237.0.64	Israel	2
5.102.196.13	147.237.76.26	Israel	5
5.102.233.237	147.237.76.134	Israel	2
5.102.234.190	147.237.76.26	Israel	10
5.102.254.76	147.237.76.26	Israel	2
5.102.254.219	147.237.0.64	Israel	2
13.82.25.17	147.237.0.23	United States	1
13.82.25.17	147.237.0.23	United States	1
13.82.25.17	147.237.9.124	United States	1
13.82.25.17	147.237.9.124	United States	1
13.82.25.17	147.237.72.231	United States	1
13.82.25.17	147.237.76.192	United States	1
13.82.25.17	147.237.76.192	United States	1
13.92.100.128	147.237.1.213	United States	1
13.92.100.128	147.237.1.213	United States	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Message	Device Action	Count
109.65.249.111	147.237.76.174	Israel	map.govmap.gov.il	drop	1362
212.150.133.231	147.237.77.115	Israel	agmon.tehila.gov.il	drop	732
169.0.178.151	147.237.0.194	South Africa		drop	560
79.183.32.30	147.237.76.239	Israel	egius.gov.il	drop	419
189.23.85.130	147.237.76.32	Brazil	EmbassiesRedirect	monitor	380
66.249.78.37	147.237.0.194	United States		drop	288
109.64.32.145	147.237.72.103	Israel	land.gov.il	drop	264
195.200.205.2	147.237.76.139	Israel	call.health.gov.il	drop	252
31.154.150.203	147.237.0.64	Israel	mof.gov.il	monitor	245
164.138.127.156	147.237.72.103	Israel	land.gov.il	drop	196
192.116.245.249	147.237.72.103	Israel	land.gov.il	drop	189
40.77.167.0	147.237.0.194	United States		drop	177
85.130.251.127	147.237.72.167	Israel	ishurim.aka.idf.il	drop	126
8.37.225.72	147.237.76.106	United States	mfa.gov.il	reject	120
8.37.225.72	147.237.76.106	United States	mfa.gov.il	monitor	120
109.64.178.11	147.237.72.103	Israel	land.gov.il	drop	120
109.160.164.111	147.237.77.90	Israel	govmap.gov.il	drop	117
79.180.36.214	147.237.72.103	Israel	land.gov.il	drop	117
109.67.189.229	147.237.76.239	Israel	egius.gov.il	drop	108
85.250.4.250	147.237.76.239	Israel	egius.gov.il	drop	105
149.88.199.199	147.237.76.106	Israel	mfa.gov.il	monitor	104
40.77.167.86	147.237.0.194	United States		drop	102
149.88.136.38	147.237.72.103	Israel	land.gov.il	drop	98
157.55.39.75	147.237.0.194	United States		drop	96
185.120.126.24	147.237.72.103	Israel	land.gov.il	drop	96
213.8.204.14	147.237.76.239	Israel	egius.gov.il	drop	96
213.224.20.54	147.237.76.106	Belgium	mfa.gov.il	monitor	95
87.71.98.145	147.237.72.103	Israel	land.gov.il	drop	87
192.116.160.223	147.237.76.241	Israel	tmichot.gov.il	drop	84
87.71.67.23	147.237.72.103	Israel	land.gov.il	drop	84
66.249.78.44	147.237.0.194	United States		drop	81
79.181.130.69	147.237.72.103	Israel	land.gov.il	drop	81
79.177.2.184	147.237.0.194	Israel		drop	78
80.178.215.172	147.237.76.241	Israel	tmichot.gov.il	drop	78
201.28.116.118	147.237.76.32	Brazil	EmbassiesRedirect	monitor	78
109.64.204.149	147.237.72.103	Israel	land.gov.il	drop	78
195.235.52.97	147.237.0.121	Spain		drop	78
87.71.31.243	147.237.76.239	Israel	egius.gov.il	drop	78
62.90.143.84	147.237.72.103	Israel	land.gov.il	drop	78
79.183.238.194	147.237.76.239	Israel	egius.gov.il	drop	78
95.213.218.142	147.237.76.106	Russian Federation	mfa.gov.il	reject	76
95.213.218.142	147.237.76.106	Russian Federation	mfa.gov.il	monitor	76
2.53.20.37	147.237.76.174	Israel	map.govmap.gov.il	drop	75
8.29.198.26	147.237.0.194	United States		drop	72
217.132.148.165	147.237.76.239	Israel	egius.gov.il	drop	72
93.173.232.72	147.237.76.239	Israel	egius.gov.il	drop	72
109.160.168.11	147.237.76.239	Israel	egius.gov.il	drop	72
65.19.138.33	147.237.0.194	United States		drop	72
85.64.125.228	147.237.76.239	Israel	egius.gov.il	drop	72
109.65.226.2	147.237.76.239	Israel	egius.gov.il	drop	72

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Sites	Name	Device Action
2.53.6.78	147.237.72.26	Israel	1	Distributed Unauthorized URL Access on 147.237.72.26/library.asp	Block
2.53.6.78	147.237.76.192	Israel	2	Distributed _vti_	Block
2.53.7.112	147.237.76.139	Israel	1	Distributed Unauthorized URL Access on call.gov.il/infocenter/apps/infocenter/custom/components/content/apps/infocenter/custom/components/content/c_autofill_mobile.jsp	Block
2.53.7.112	147.237.76.139	Israel	1	Distributed Unauthorized URL Access on call.gov.il/infocenter/apps/infocenter/custom/pages/mobile/apps/infocenter/custom/components/content/c_autofill_mobile.jsp	Block
2.53.8.128	147.237.77.90	Israel	1	Distributed Illegal Parameter Encoding	None
2.53.26.183	147.237.77.90	Israel	1	Distributed Illegal Parameter Encoding	None
2.53.29.136	147.237.72.51	Israel	1	SSL Untraceable Connection - Open Mode	None
2.53.36.26	147.237.77.230	Israel	1	Too Many Headers per Response - 26 Headers	Block
2.53.36.227	147.237.76.43	Israel	2	Distributed _vti_	Block
2.53.57.177	147.237.77.90	Israel	1	Distributed Illegal Parameter Encoding	None
2.53.137.215	147.237.76.139	Israel	3	Distributed Unauthorized URL Access on call.gov.il/infocenter/apps/infocenter/custom/pages/mobile/apps/infocenter/custom/components/content/c_autofill_mobile.jsp	Block
2.53.137.215	147.237.76.139	Israel	2	Unauthorized URL Access to call.gov.il/infocenter/apps/infocenter/custom/components/content/apps/infocenter/custom/components/content/c_autofill_mobile.jsp	Block
2.53.149.136	147.237.77.90	Israel	1	Distributed Illegal Parameter Encoding	None
2.53.154.86	147.237.76.18	Israel	1	Multiple Untraceable SSL Sessions from 2.53.154.86 (Open Mode)	None
2.53.154.86	147.237.76.18	Israel	1	SSL Untraceable Connection - Open Mode	None
2.53.154.86	147.237.77.199	Israel	1	Untraceable SSL Sessions: Open Mode	None
2.53.174.200	147.237.77.238	Israel	5	Distributed _vti_	Block
2.53.188.217	147.237.76.42	Israel	1	Parameter Type Violation ct100\$ContentPlaceholder1\$btnSend.x in www.refua.atal.idf.il/1518-he/refuah.aspx	Block
2.55.39.193	147.237.1.42	Israel	1	Unknown Parameter NewPassword in m.milum-ishi.aka.idf.il/	None
2.55.44.17	147.237.76.139	Israel	1	Distributed Unauthorized URL Access on call.gov.il/infocenter/apps/infocenter/custom/components/content/apps/infocenter/custom/components/content/c_autofill_mobile.jsp	Block
2.55.44.17	147.237.76.139	Israel	1	Distributed Unauthorized URL Access on call.gov.il/infocenter/apps/infocenter/custom/pages/mobile/apps/infocenter/custom/components/content/c_autofill_mobile.jsp	Block
2.55.136.7	147.237.1.105	Israel	1	Distributed Abnormally Long Request	None
2.87.103.86	147.237.76.106	Greece	1	Distributed PHP Attempt	Block
2.216.192.89	147.237.77.18	United Kingdom	2	Distributed _vti_	Block
5.9.59.79	147.237.72.42	Germany	7	Distributed PHP Attempt	Block
5.9.59.79	147.237.72.42	Germany	3	Multiple signatures from 5.9.59.79	Block
5.22.130.109	147.237.77.90	Israel	1	Distributed Illegal Parameter Encoding	None
5.22.131.41	147.237.76.43	Israel	58	Distributed _vti_	Block
5.22.135.118	147.237.77.209	Israel	1	Distributed _vti_	Block
5.22.135.210	147.237.77.130	Israel	4	Distributed Unauthorized Http Methods	Block
5.28.135.19	147.237.77.18	Israel	2	Distributed _vti_	Block
5.28.148.193	147.237.0.114	Israel	3	Distributed Malformed JSON Message	None
5.28.148.193	147.237.0.114	Israel	4	Distributed Unauthorized URL Access on ica.justice.gov.il/documents/getdocumentlist/	Block
5.28.163.81	147.237.72.176	Israel	5	Distributed Suspicious Response Code - With Gateway	Block
5.28.172.160	147.237.77.90	Israel	1	Distributed Illegal Parameter Encoding	None
5.28.184.245	147.237.76.139	Israel	1	Distributed Unauthorized URL Access on call.health.gov.il/infocenter/apps/infocenter/custom/pages/mobile/apps/infocenter/custom/components/content/c_autofill_mobile.jsp	Block
5.28.184.245	147.237.76.139	Israel	1	Unauthorized URL Access to call.health.gov.il/infocenter/apps/infocenter/custom/components/content/apps/infocenter/custom/components/content/c_autofill_mobile.jsp	Block
5.28.187.147	147.237.77.130	Israel	1	_vti_	Block
5.29.1.126	147.237.76.26	Israel	1	Distributed Unauthorized Http Methods	Block
5.29.1.126	147.237.76.26	Israel	1	Distributed Unauthorized URL Access on index.justice.gov.il/error.htm	Block
5.29.8.39	147.237.77.173	Israel	2	Distributed Unauthorized URL Access on archive.piba.gov.il/russian/pages/default.aspx	Block
5.29.22.118	147.237.76.43	Israel	59	Distributed _vti_	Block
5.29.77.183	147.237.77.18	Israel	1	Distributed Unauthorized HTTP Method	Block
5.29.115.58	147.237.76.43	Israel	1	Distributed _vti_	Block
5.29.160.145	147.237.76.43	Israel	2	Distributed _vti_	Block
5.29.189.74	147.237.77.173	Israel	5	Distributed Unauthorized URL Access on archive.piba.gov.il/russian/pages/default.aspx	Block
5.29.234.163	147.237.77.90	Israel	1	Distributed Illegal Parameter Encoding	None
5.29.238.214	147.237.76.134	Israel	2	Distributed _vti_	Block
5.100.253.184	147.237.0.46	Israel	1	Distributed Unauthorized URL Access on survey.gov.il/sites/default/files/css/css_r-slmej6rjbanqclue8ngyb_qxwbfaw582itdgl3rbq.css	None
5.100.253.184	147.237.0.46	Israel	5	Multiple Unauthorized URL Access from 5.100.253.184	None