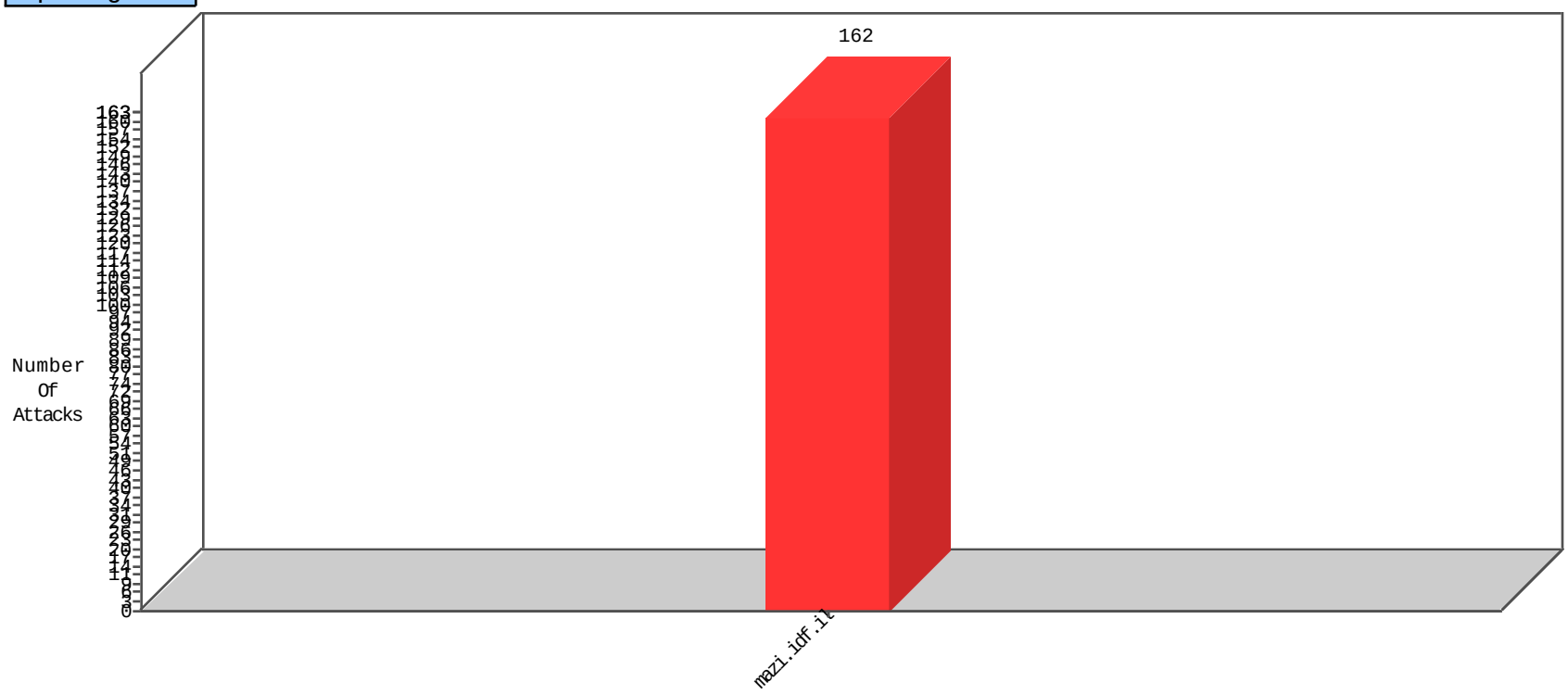
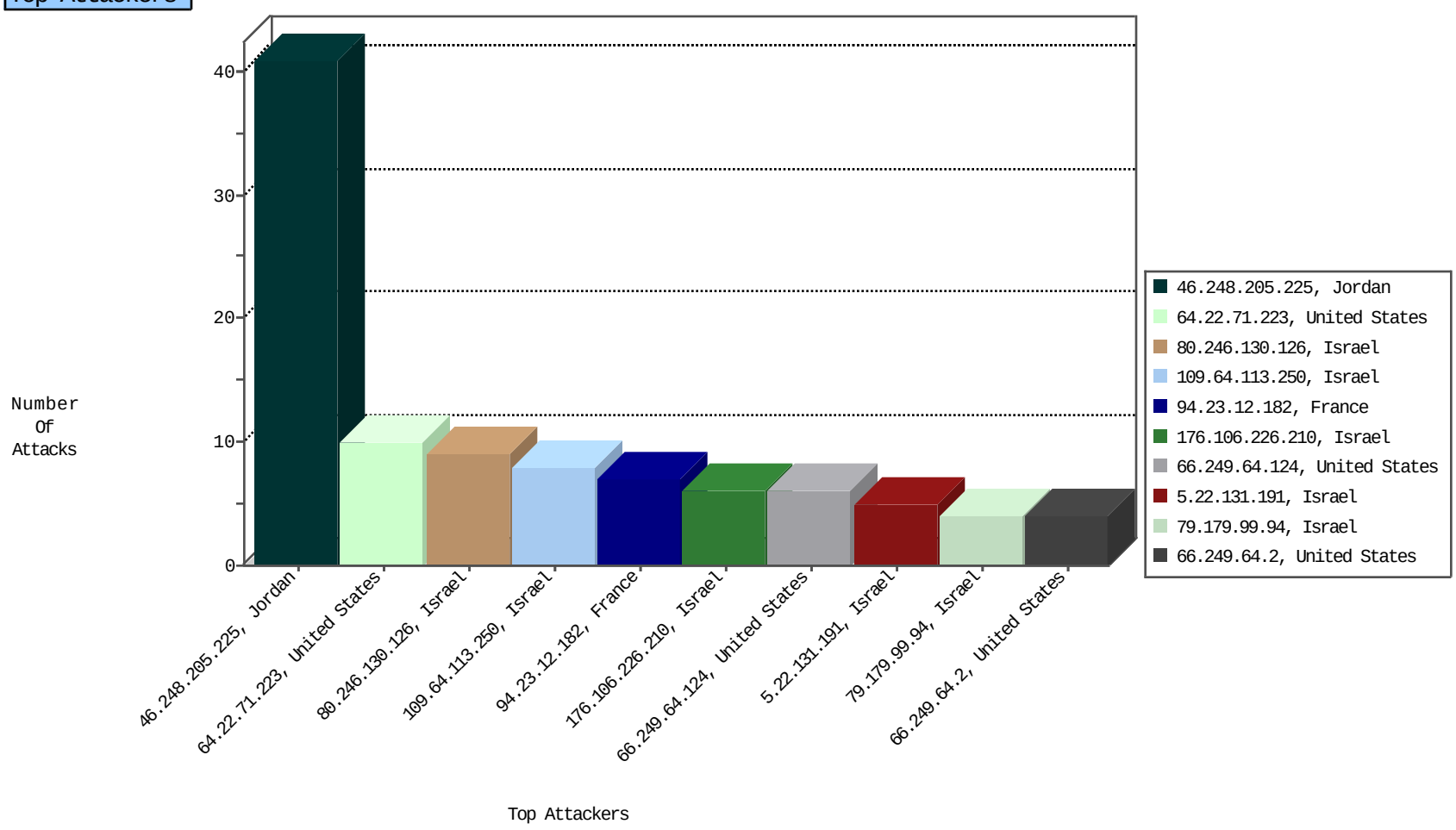
11-27-2015 to 11-28-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



11-27-2015 to 11-28-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
109.64.113.250	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	8
64.22.71.223	United States	147.237.77.17	mazi.idf.il	JLM_Purple_Con_Limit_Http	drop	DP-Tehila	3
46.248.205.225	Jordan	147.237.77.17	mazi.idf.il	block-sp-traf1	drop	BBL-Frankfurt	1

11-27-2015 to 11-28-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
46.248.205.225	Jordan	147.237.77.17	mazi.idf.il	C017: HTTP: Malicous UserAgent FOCA	Block	37
188.165.15.84	France	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	2
46.248.205.225	Jordan	147.237.77.17	mazi.idf.il	10714: HTTP: Netsparker Security Scanner	Block	1

11-27-2015 to 11-28-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.64.124	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	6
66.249.64.2	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	4
118.71.153.234	Vietnam	147.237.77.17	mazi.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	2
59.45.79.117	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
77.109.38.223	Ukraine	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.134	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 4096	1
199.101.186.178	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 4096	1
61.191.190.47	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
114.35.44.25	Taiwan	147.237.77.17	mazi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.136.130.194	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.178	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1

11-27-2015 to 11-28-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
64.22.71.223	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4705
64.22.71.223	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	2305
64.22.71.223	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	2304
87.68.77.9	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	93
79.181.108.249	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
185.120.126.61		147.237.77.17	mazi.idf.i	drop	SAM rule	drop	36
46.19.85.104	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	25
46.19.85.104	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
79.179.163.239	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
208.115.111.75	United States	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	25
46.19.86.185	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
185.3.144.30	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	17
213.57.129.238	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
77.126.21.40	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
5.102.254.151	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
176.106.227.229	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
213.57.143.209	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
85.237.234.228	Slovakia	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.220	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.249	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.121.158.216	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.14	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.220	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.14	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.91	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
87.69.228.156	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.155	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
84.94.200.241	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.197	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
94.230.86.161	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
79.179.23.163	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
2.54.150.214	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
185.3.144.168	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.28	United Kingdom	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
185.120.125.18		147.237.77.17	mazi.idf.i	drop	SAM rule	drop	2
84.201.138.23	Russian Federation	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
213.57.128.231	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
77.127.147.151	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.107	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
157.55.39.131	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.120	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
139.162.146.245	Netherlands	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
87.69.44.48	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
216.243.31.2	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.52.42.158	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
64.22.71.223	United States	147.237.77.17	mazi.idf.i	Network Quota Violation	Network quota was exceeded	monitor	1
178.79.182.42	United Kingdom	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.220	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.56	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.54	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
80.246.130.126	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	9
64.22.71.223	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 64.22.71.223	Block	7
5.22.131.191	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/ufi/reaction/	Block	5
94.23.12.182	France	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	3
46.121.136.121	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/templates/newslist/undefined	Block	2
84.108.249.89	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	2
176.106.226.210	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	2
94.23.12.182	France	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/index.php	Block	2
79.179.99.94	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	2
157.55.39.51	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/14-8335-he	Block	2
31.168.90.25	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
176.106.226.210	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 176.106.226.210	Block	2
109.66.115.46	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	2
62.128.48.122	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/images/transvideocounter.gif	Block	2
176.106.226.210	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
79.177.28.179	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
66.249.64.124	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8333-he	Block	1
141.212.121.208	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/	Block	1
95.86.66.163	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
2.52.42.158	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/1603-15076-he/dover.aspx	Block	1
84.229.29.61	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 84.229.29.61	Block	1
79.179.99.94	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
185.3.144.30	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/favicon.ico	Block	1
157.55.39.58	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/14-4980-he	Block	1
66.249.64.180	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6752-10419-he/igf.aspx	Block	1
109.186.185.45	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
40.77.167.95	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
94.23.12.182	France	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 94.23.12.182	Block	1
176.106.226.210	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
79.177.28.179	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
66.249.64.175	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/	Block	1
141.212.122.112	United States	147.237.77.17	mazi.idf.i	Multiple Malformed URL from 141.212.122.112	Block	1
109.66.30.143	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
46.248.205.225	Jordan	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 46.248.205.225	Block	1
87.68.77.9	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3848-5183-he/igf.aspx	Block	1
79.179.133.236	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
207.46.13.109	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/113-9697-he/igf.aspx	Block	1
66.249.64.185	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/165-7902-he/igf.aspx	Block	1
66.249.64.8	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/700-he/bayabashaarchive.aspx	Block	1
109.186.185.45	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/xmlrpc.php	Block	1
46.116.106.18	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
84.109.38.222	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
180.76.15.29	China	147.237.77.17	mazi.idf.i	Suspicious Response Code	Block	1
66.249.64.175	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
109.66.30.143	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/xmlrpc.php	Block	1
46.248.205.225	Jordan	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-he/igf.aspx"	Block	1
94.23.12.182	France	147.237.77.17	mazi.idf.i	Distributed Admin Blocking	Block	1
79.179.133.236	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
207.46.13.136	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6221-9268-he/igf.aspx	Block	1
66.249.64.185	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.64.16	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/newslist/undefined	Block	1
118.71.153.234	Vietnam	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/shared/clientscripts/}function bp(a,b){b.src	Block	1
94.230.86.161	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
46.116.106.18	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 46.116.106.18	Block	1
84.229.29.61	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
46.116.106.18	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 46.116.106.18	Block	1
84.229.29.61	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
185.3.144.30	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
79.179.99.94	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 79.179.99.94	Block	1
66.249.64.180	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3697-9051-he/igf.aspx	Block	1
157.55.39.58	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 157.55.39.58	Block	1
40.77.167.34	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files	Block	1