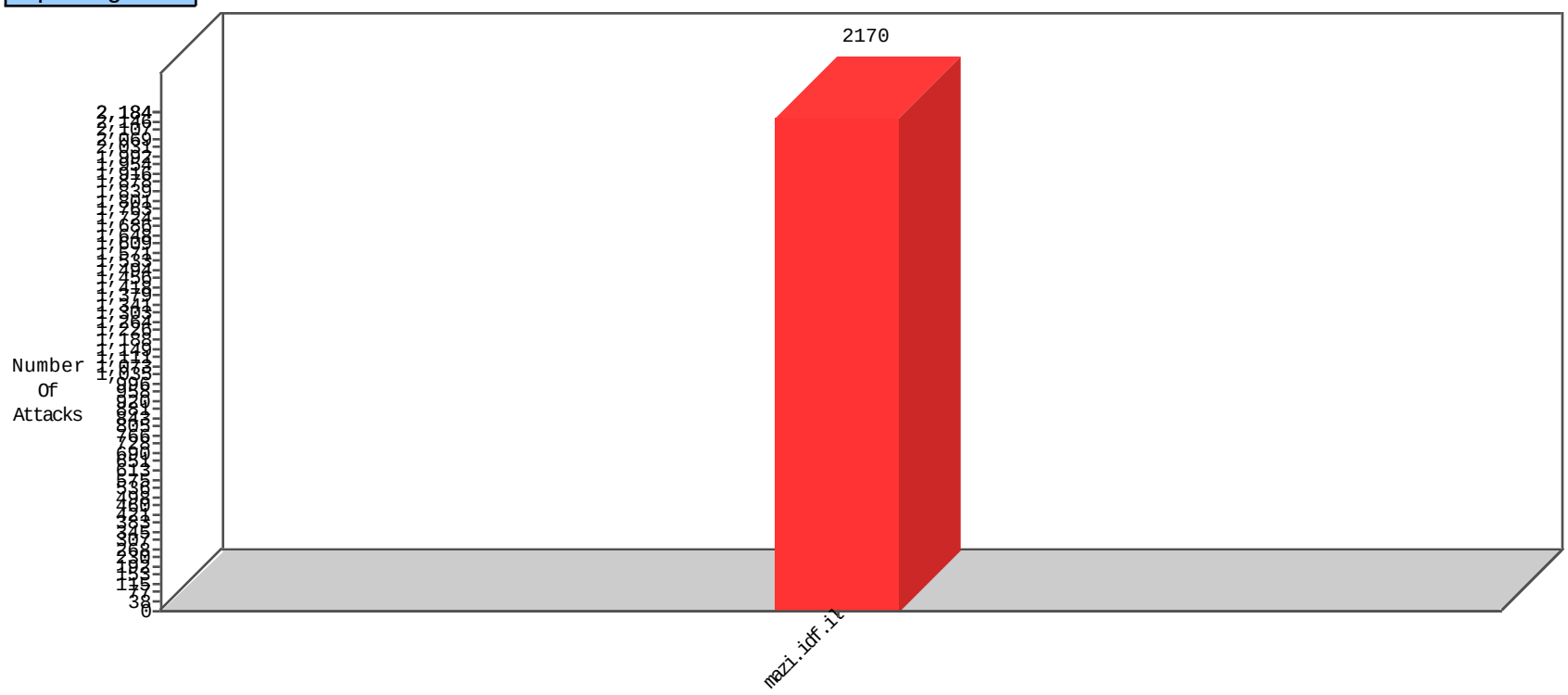
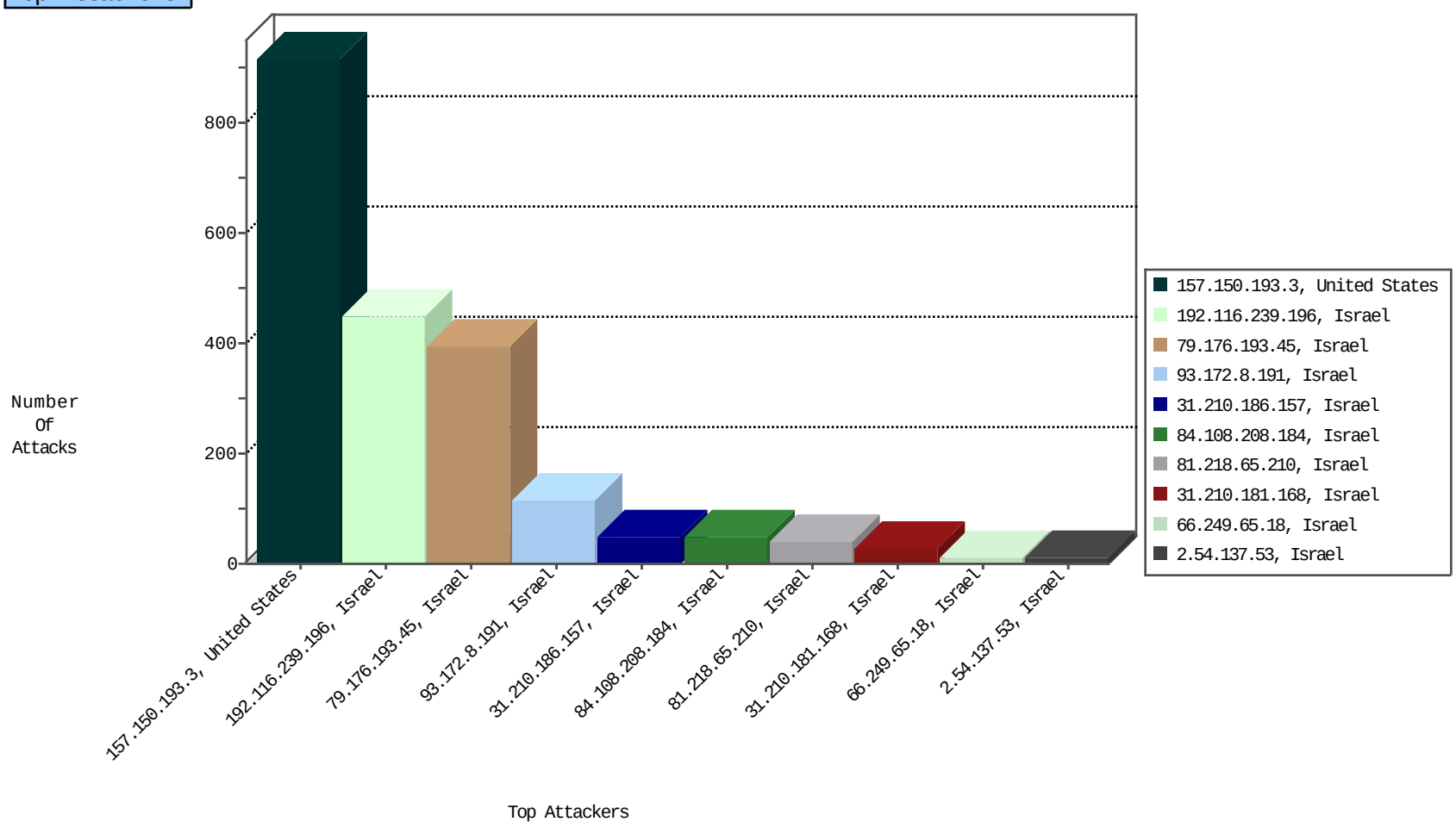
03-14-2016 to 03-15-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



03-14-2016 to 03-15-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
157.150.193.3	United States	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	NetV-London	918
81.218.65.210	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	39
37.26.146.224	Israel	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	NetV-London	1
103.235.242.51	China	147.237.77.17	mazi.idf.il	L4 Source or Dest Port Zero	drop	BBL-Frankfurt	1
159.104.163.17	United Kingdom	147.237.77.17	mazi.idf.il	Invalid TCP Flags	drop	NetV-London	1
159.104.163.18	United Kingdom	147.237.77.17	mazi.idf.il	Invalid TCP Flags	drop	NetV-London	1

03-14-2016 to 03-15-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
192.116.239.196	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	450
79.176.193.45	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	394
93.172.8.191	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	114
31.210.186.157	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	50
84.108.208.184	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	46
31.210.181.168	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	26
66.249.65.18	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
2.54.137.53	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
79.177.204.115	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
82.193.127.15	Ukraine	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	5
66.249.65.18	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
62.210.115.133	France	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	4
72.13.87.202	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
37.46.38.40	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
95.86.114.209	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
77.125.159.35	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
62.219.96.2	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
176.9.131.69	Germany	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
84.94.223.111	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.19.85.29	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
212.76.106.72	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.64.21.222	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
65.55.210.70	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
69.30.198.242	United States	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
46.19.85.149	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
217.132.53.119	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.67.7.148	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.30.24.212	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
157.55.39.193	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
207.46.13.10	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
10.0.0.7		147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
66.249.65.22	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

03-14-2016 to 03-15-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.93.63	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.18	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
198.20.69.98	United States	147.237.77.17	mazi.idf.il	ET DROP Dshield Block Listed Source	1
211.149.156.87	China	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
58.253.96.122	China	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
175.100.5.215	Cambodia	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
208.80.155.214	United States	147.237.77.17	mazi.idf.il	Tehila - Perl LWP with fake user agent	1
58.253.96.122	China	147.237.77.17	mazi.idf.il	ET SCAN NMAP -f -sS	1
58.253.96.122	China	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 2048	1

03-14-2016 to 03-15-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
46.19.85.139	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	49
46.19.85.139	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	49
46.19.85.150	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
46.19.85.150	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	36
46.19.85.100	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
46.19.85.16	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	25
46.19.85.16	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
46.19.85.100	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	25
46.19.85.34	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
185.24.205.87	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.19.85.34	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
5.28.131.167	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	9
94.228.34.248	United Kingdom	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
81.218.251.252	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
5.28.131.167	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
94.230.86.248	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.116.26.121	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.64.176.44	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
199.203.215.1	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
87.71.58.37	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.121.96.55	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
91.200.12.136	Ukraine	147.237.77.17	mazi.idf.il	drop	SAM rule	drop	4
85.64.176.44	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.116.239.196	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
5.22.131.76	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.221	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
84.94.47.122	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
192.116.239.196	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.187.50	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
157.150.193.3	United States	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.94.32.197	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.176.193.45	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
94.228.34.248	United Kingdom	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
2.54.161.2	Israel	147.237.77.17	mazi.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
82.193.127.15	Ukraine	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.3.147.47	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
2.52.187.50	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
64.125.239.210	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
157.55.39.193	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
85.65.199.133	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.243.31.2	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.46.39.123	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
84.94.115.189	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
193.105.134.220	Sweden	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.12.51.17	Romania	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.75	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.52.2.39	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.121.96.55	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.75	United States	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
89.138.93.112	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

03-14-2016 to 03-15-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
95.86.114.209	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	7
95.86.125.75	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	3
70.187.177.167	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	2
37.46.39.123	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master$ucHeader$ucSearchControl$txtSearch in www.mazi.idf.il/4384-he/igf.aspx	Block	2
109.253.147.155	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage	Block	2
65.208.151.115	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/shared/usercontrols/banners/mazi.idf.il/113-10481-he/piwik.php	Block	1
149.78.114.10	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/xmlrpc.php	Block	1
104.131.147.112	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5216-he/igf.aspx	Block	1
37.26.147.166	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/2061.jpg	Block	1
117.78.13.29	China	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-he	Block	1
94.230.86.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
66.249.65.18	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/general/ה	Block	1
157.55.39.193	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/ موقع	Block	1
109.64.188.204	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
79.176.210.158	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
141.212.122.64	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to /x	Block	1
68.180.229.109	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 68.180.229.109	Block	1
178.216.200.48	Poland	147.237.77.17	mazi.idf.i	Unauthorized URL Access to testp1.piwo.pila.pl/testproxy.php	Block	1
109.64.188.204	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
79.176.210.158	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
65.208.151.115	United States	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
149.78.114.10	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
68.180.229.109	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8330-he	Block	1
5.255.253.65	Russian Federation	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5580-7562-he/igf.asp	Block	1
213.177.107.202	Russian Federation	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-he/	Block	1
84.94.47.122	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5187-he/igf.aspx	Block	1

03-14-2016 to 03-15-2016