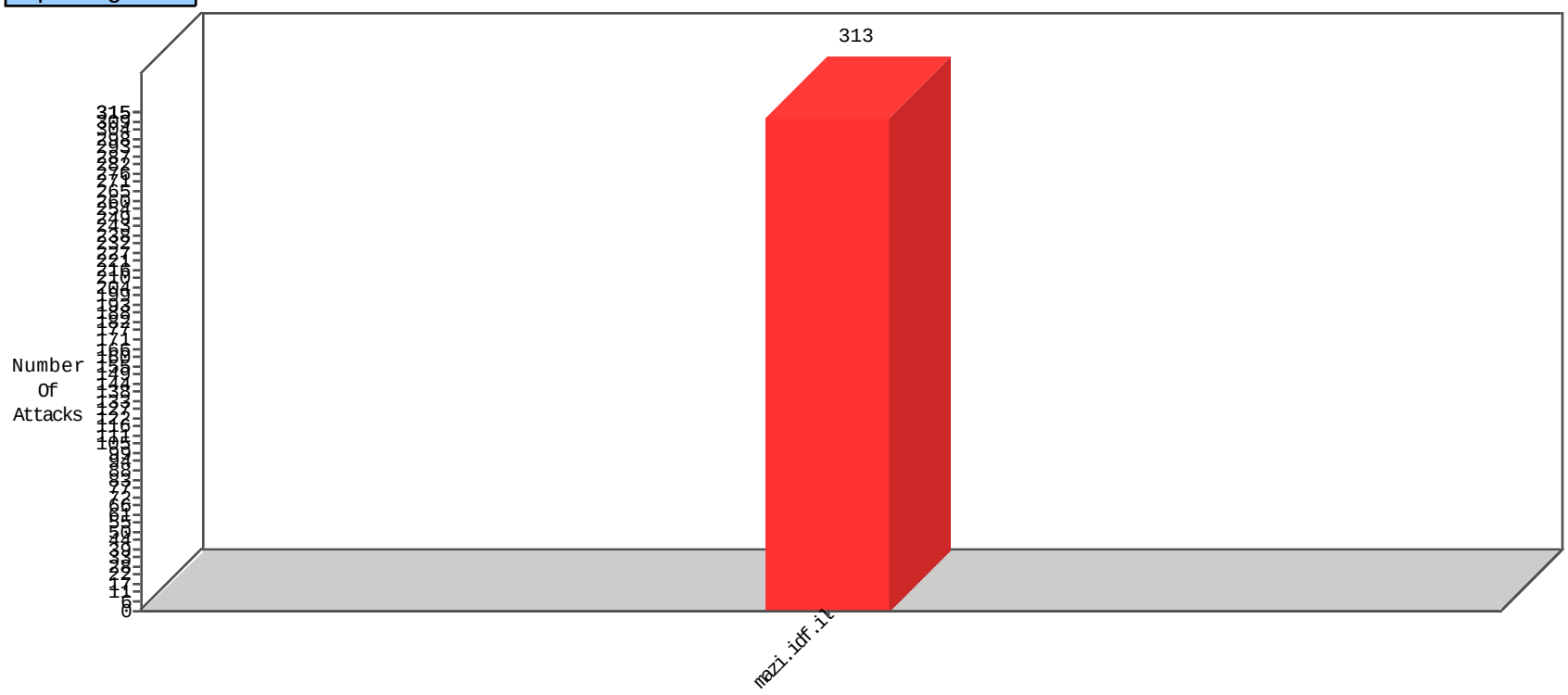
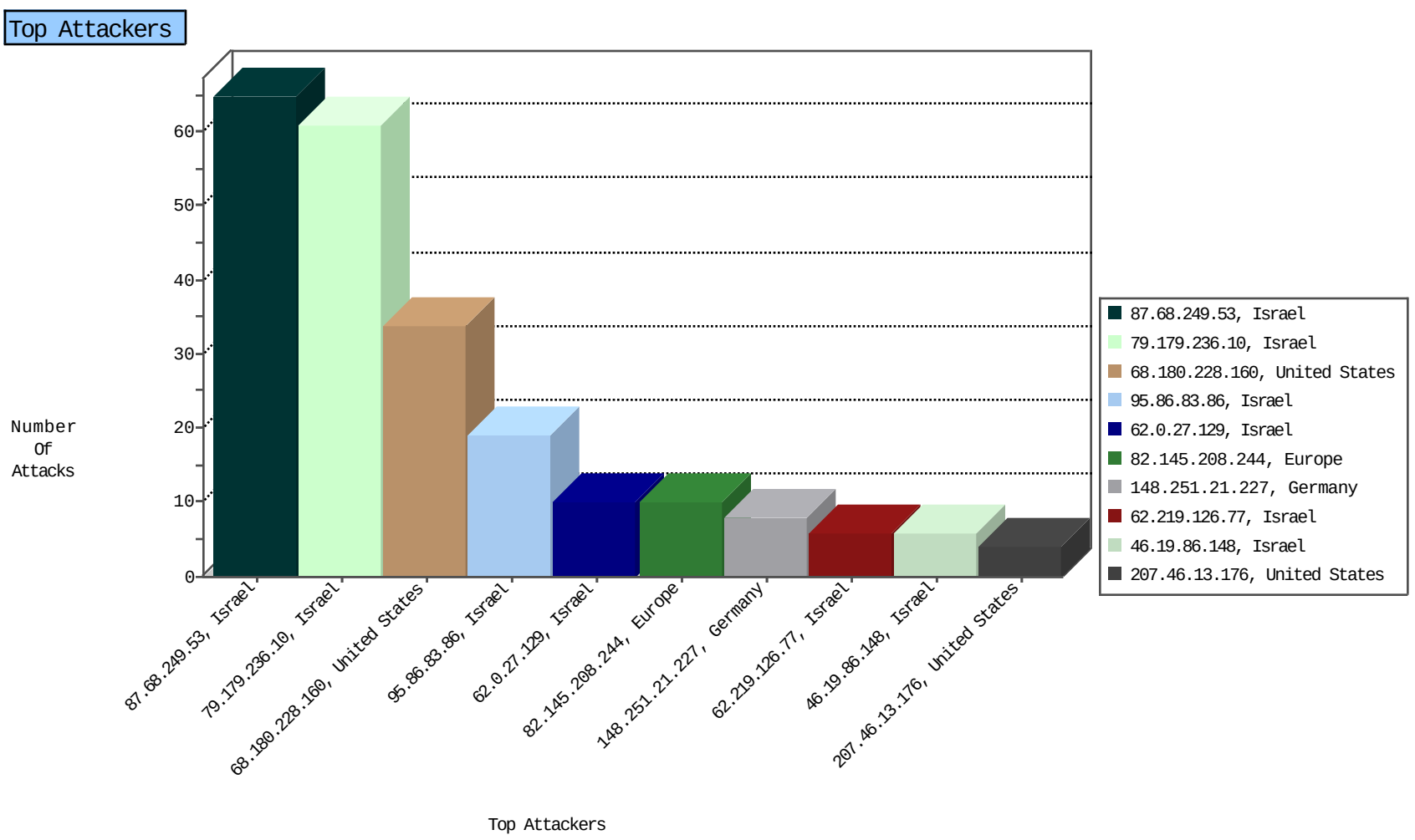
03-02-2016 to 03-03-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



03-02-2016 to 03-03-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
82.145.208.244	Europe	147.237.77.17	mazi.idf.il	Block_Ip_Web_In	drop	NetV-London	10
54.72.182.187	Ireland	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	3
52.53.222.9	United States	147.237.77.17	mazi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
164.132.54.194	Italy	147.237.77.17	mazi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
184.105.139.120	United States	147.237.77.17	mazi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
198.204.249.50	United States	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	1

03-02-2016 to 03-03-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
87.68.249.53	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	65
79.179.236.10	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	61
68.180.228.160	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	34
95.86.83.86	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
62.0.27.129	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
46.19.86.148	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
207.46.13.176	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
62.90.202.217	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
144.76.12.75	Germany	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
62.210.170.165	France	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
207.46.13.192	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
77.127.90.53	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
107.170.68.76	United States	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.75.26	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
213.8.204.72	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
195.154.187.115	France	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
131.253.25.166	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.75.34	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
151.80.31.153	Italy	147.237.77.17	mazi.idf.il	C1000146: HTTP: AhrefBot crawler	Block	2
31.154.94.18	Israel	147.237.77.17	mazi.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	1
151.80.31.154	Italy	147.237.77.17	mazi.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.150	Italy	147.237.77.17	mazi.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
185.80.220.24		147.237.77.17	mazi.idf.il	0543: HTTP: php.cgi Access	Block	1
151.80.31.151	Italy	147.237.77.17	mazi.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

03-02-2016 to 03-03-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.102.9.101	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.5	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
174.37.194.144	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
66.249.75.18	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
45.32.49.30		147.237.77.17	mazi.idf.il	ET SCAN NMAP -f -sS	1
45.32.49.30		147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 2048	1
137.226.113.7	Germany	147.237.77.17	mazi.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	1

03-02-2016 to 03-03-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	64
192.243.55.135	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	64
192.243.55.130	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	60
192.243.55.138	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	60
192.243.55.133	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	52
192.243.55.132	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	51
192.243.55.136	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	51
192.243.55.130	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	49
192.243.55.129	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	46
192.243.55.132	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	45
192.243.55.131	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	42
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	41
192.243.55.138	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	40
192.243.55.130	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	40
192.243.55.137	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	39
46.19.85.52	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	37
192.243.55.132	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	37
192.243.55.131	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	37
192.243.55.129	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
46.19.85.52	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	36
192.243.55.135	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	34
192.243.55.137	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	34
192.243.55.136	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	33
192.243.55.131	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	32
192.243.55.130	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	32
192.243.55.133	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	31
192.243.55.129	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	31
192.243.55.138	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	30
192.243.55.136	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
192.243.55.132	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	28
192.243.55.130	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	27
192.243.55.133	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	27
46.19.85.159	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
192.243.55.132	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	26
192.243.55.135	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	26
46.19.85.7	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
192.243.55.131	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
46.19.85.159	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	25
46.19.85.7	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	25
192.243.55.129	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	24
192.243.55.131	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	24
2.52.56.43	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	23
192.243.55.138	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	22
192.243.55.137	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
192.243.55.138	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	20
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	20
192.243.55.129	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	20
192.243.55.137	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	18

03-02-2016 to 03-03-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
148.251.21.227	Germany	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 148.251.21.227	Block	7
62.219.126.77	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	6
95.86.83.86	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/images/transvideocounter.gif	Block	3
95.86.112.221	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/images/transvideocounter.gif	Block	2
46.19.85.153	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage	Block	2
68.180.230.40	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
192.243.55.137	Dominica	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 192.243.55.137	Block	1
66.249.69.2	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
185.82.203.241		147.237.77.17	mazi.idf.i	Parameter Type Violation TabNum in mazi.idf.il/4277-he/igf.aspx	Block	1
5.28.167.149	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master$ucHeader$ucSearchControl$txtSearch in www.mazi.idf.il/671-he/igf.aspx	Block	1
79.177.244.130	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
207.46.13.109	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5212-6318-he/igf.aspx	Block	1
66.249.93.103	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1
54.213.177.200	United States	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in Method	Block	1
192.243.55.131	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-7713-he	Block	1
176.228.71.8	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
77.237.138.202	Czech Republic	147.237.77.17	mazi.idf.i	Unauthorized Method HEAD for /	Block	1
192.243.55.137	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8346-he	Block	1
66.249.75.129	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
40.77.167.55	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/sip_storage/files	Block	1
192.243.55.129	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8333-he	Block	1
148.251.21.227	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/ד×Þ×	Block	1
79.181.51.141	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
207.46.13.176	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/templates/newslist/undefined	Block	1
66.249.93.107	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
54.213.177.200	United States	147.237.77.17	mazi.idf.i	NULL Character in Method	Block	1
192.243.55.135	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-7712-he	Block	1
177.64.198.101	Brazil	147.237.77.17	mazi.idf.i	Admin Blocking	Block	1
79.143.180.15	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5579-7564-he/mailto:igf@idf.gov.il	Block	1
198.20.69.74	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.75.129	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
40.77.167.88	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/6/3376.jpg	Block	1
192.243.55.130	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-5475-he	Block	1
157.55.39.189	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5221-6391-he/igf.aspx	Block	1
80.246.130.15	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
67.194.239.33	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1
207.232.27.5	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/images/transvideocounter.gif	Block	1
192.243.55.136	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/www.idiegogo.com/projects/121440	Block	1
185.3.144.23	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1
95.86.127.23	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4450-he/igf.aspx&sa=u&ved=0ahukewipzrdszallahvptymkhfnech4qfgghmag&usg=afqjcnevz5hduuxes1hq-jtqm06zydwqsa	Block	1
79.176.223.19	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5772	Block	1
207.46.13.44	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/591-he/igf.aspx	Block	1
66.249.75.145	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
192.243.55.131	Dominica	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 192.243.55.131	Block	1
176.228.71.8	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 176.228.71.8	Block	1
87.71.22.180	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1

03-02-2016 to 03-03-2016