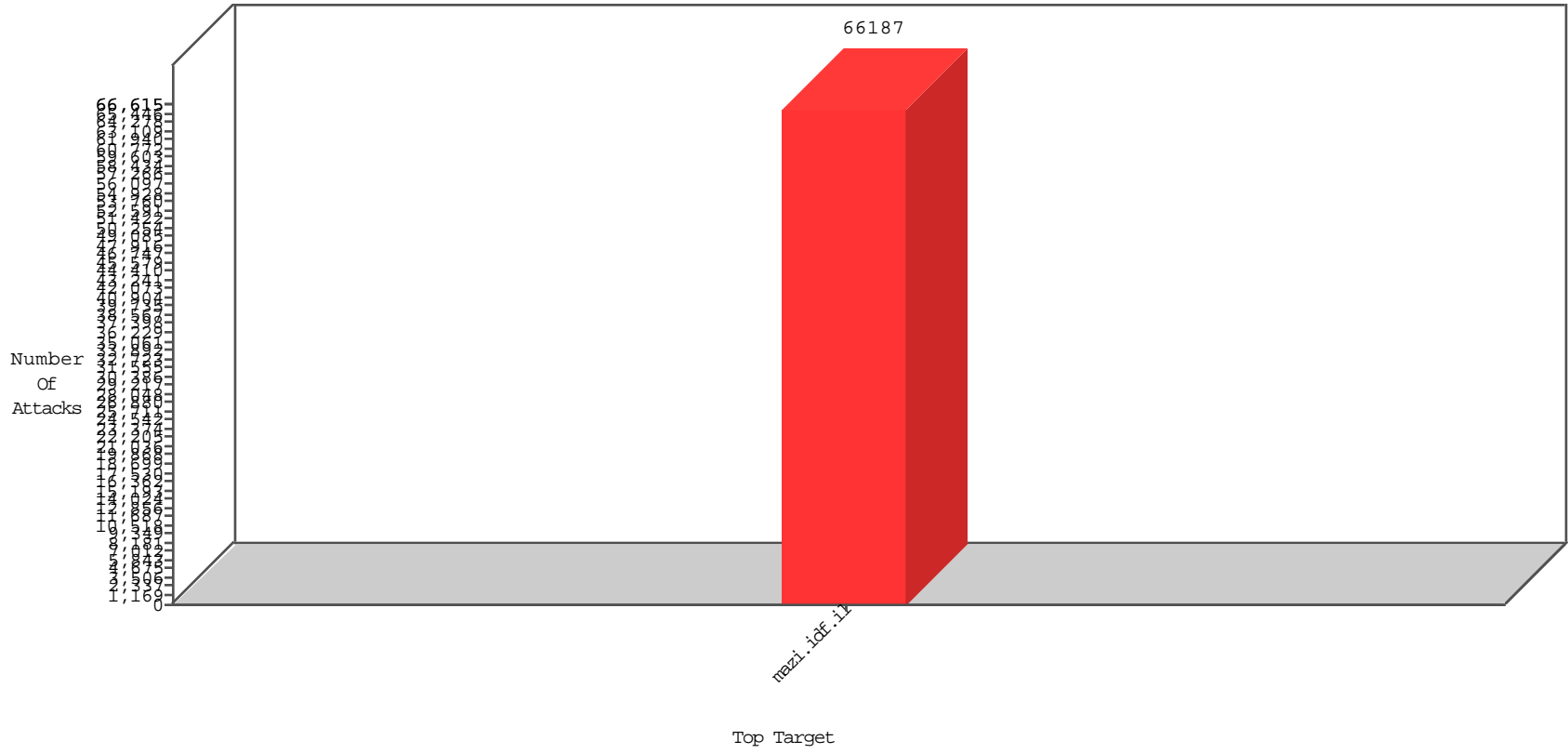


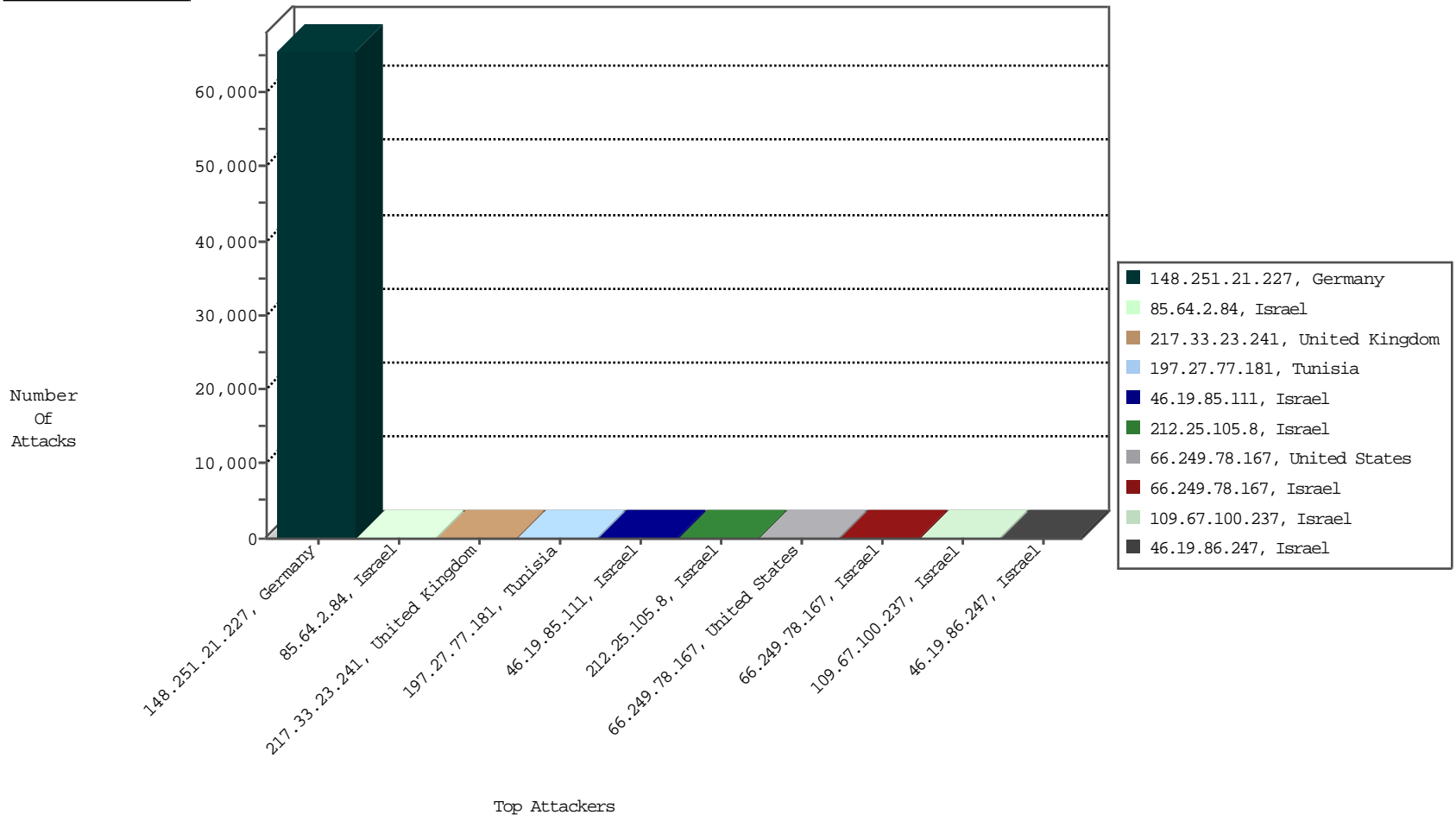
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
148.251.21.227	Germany	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	NetV-London	65739
54.72.182.187	Ireland	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	3
61.178.192.220	China	147.237.77.17	mazi.idf.il	Invalid TCP Flags	drop	NetV-London	2
179.43.144.33	Switzerland	147.237.77.17	mazi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
184.105.139.88	United States	147.237.77.17	mazi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
205.209.185.11	United States	147.237.77.17	mazi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
216.220.226.51	United States	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
66.249.75.18	Israel	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	1
81.218.56.125	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	1
170.161.102.40	United States	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	1

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
85.64.2.84	Israel	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	84
217.33.23.241	United Kingdom	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	82
46.19.85.111	Israel	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	28
212.25.105.8	Israel	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	26
66.249.78.167	Israel	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	18
109.67.100.237	Israel	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	10
46.19.86.247	Israel	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	10
66.249.78.174	Israel	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	6
66.249.78.181	Israel	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	3
151.80.31.154	Italy	147.237.77.17	mazi.idf.i	C1000146: HTTP: AhrefBot crawler	Block	3
151.80.31.151	Italy	147.237.77.17	mazi.idf.i	C1000146: HTTP: AhrefBot crawler	Block	2
84.228.252.234	Israel	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.75.18	Israel	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	2
174.34.135.242	United States	147.237.77.17	mazi.idf.i	C1000074: HTTP: majestic bot	Block	2
79.181.53.250	Israel	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	2
89.139.61.242	Israel	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	2
213.8.109.42	Israel	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	2
84.108.185.15	Israel	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.254.129.87	United Kingdom	147.237.77.17	mazi.idf.i	C1000074: HTTP: majestic bot	Block	2
173.234.153.122	United States	147.237.77.17	mazi.idf.i	C1000074: HTTP: majestic bot	Block	2
104.255.65.207		147.237.77.17	mazi.idf.i	0543: HTTP: php.cgi Access	Block	1
66.249.75.34	Israel	147.237.77.17	mazi.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	1
172.245.12.146	United States	147.237.77.17	mazi.idf.i	0543: HTTP: php.cgi Access	Block	1
151.80.31.150	Italy	147.237.77.17	mazi.idf.i	C1000146: HTTP: AhrefBot crawler	Block	1
89.216.115.6		147.237.77.17	mazi.idf.i	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	1

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.78.167	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	18
187.58.224.213	Brazil	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
187.58.224.213	Brazil	147.237.77.17	mazi.idf.il	ET SCAN NMAP -f -sS	1
187.58.224.213	Brazil	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 2048	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.78.167	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	79
79.183.62.23	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	42
66.249.78.167	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	39
2.52.5.194	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	26
37.142.153.134	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	24
37.142.153.134	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	19
212.76.127.219	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	18
109.65.99.4	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
85.130.128.51	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
212.76.127.10	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
192.115.83.5	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
148.251.21.227	Germany	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
5.102.242.136	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.5.194	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	5
5.28.133.115	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
212.76.127.44	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
5.102.241.4	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
157.55.39.68	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
188.120.148.193	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
203.133.169.220	Korea, Republic of	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
79.182.176.153	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
157.55.39.141	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.85.111	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
192.115.83.5	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	2
207.46.13.99	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
37.46.41.24	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.145.209	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
80.179.96.90	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	2
157.55.39.89	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
80.179.96.90	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
79.178.196.73	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.38.29	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
37.46.38.132	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
185.106.92.164		147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.22.135.239	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
66.249.78.174	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
46.121.81.184	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
112.215.36.143	Indonesia	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
104.45.18.178	United States	147.237.77.17	mazi.idf.i	Instant Messengers	instant messenger pattern found, application: Skype	monitor	1
208.115.113.91	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
31.210.187.106	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
84.108.33.189	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
5.29.243.118	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
79.180.110.117	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
176.13.12.198	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
2.54.47.129	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
66.249.75.18	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
149.88.83.202	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.120.154.134	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
109.66.7.21	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
197.27.77.181	Tunisia	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 197.27.77.181	Block	55
148.251.21.227	Germany	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 148.251.21.227	Block	9
95.86.105.224	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	5
172.245.12.146	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 172.245.12.146	Block	3
212.76.104.98	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	2
46.19.86.104	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage	Block	2
107.77.70.51	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/images/transvideocounter.gif	Block	1
66.249.78.242	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.78.17	United States	147.237.77.17	mazi.idf.i	Parameter Type Violation Back in igf.idf.il/6053-he/igf.aspx	Block	1
197.27.77.181	Tunisia	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5069-he/igf'.aspx	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in URL • •ü ú ~wvç•[[#15]]@.. 0	Block	1
66.249.69.2	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5479-he/igf.aspx	Block	1
5.102.242.38	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4637-5227-he/igf.aspx	Block	1
80.178.203.105	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
66.249.78.242	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/3849-5035-he/igf.aspx	Block	1
66.249.75.168	United States	147.237.77.17	mazi.idf.i	Parameter Type Violation TabNum in igf.idf.il/4941-he/igf.aspx	Block	1
172.245.12.146	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/cgi-bin/php	Block	1
157.55.39.89	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-8334-he	Block	1
46.19.86.112	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/2061.jpg	Block	1
107.167.97.208	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/2061.jpg	Block	1
66.249.78.248	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6057-he/igf.aspx	Block	1
207.46.13.70	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-8347-he	Block	1
66.249.78.77	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Malformed URL • •ü ú ~wvç•[[#15]]@.. 0	Block	1
66.249.75.18	United States	147.237.77.17	mazi.idf.i	Parameter Type Violation PageNum in mazi.idf.il/5013-he/igf.aspx	Block	1
37.142.153.134	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/templates/general/	Block	1
148.251.21.227	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/113-11581-he/.aspx	Block	1
80.246.133.140	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master\$ucHeader\$ucSearchControl\$txtSearch in www.mazi.idf.il/14-he/igf.aspx	Block	1
66.249.78.242	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6107-he/igf.aspx	Block	1
66.249.78.3	United States	147.237.77.17	mazi.idf.i	Parameter Type Violation PageNum in igf.idf.il/165-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
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in Method Söj~	Block	1
64.251.27.99	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to /robots.txt	Block	1
107.167.103.126	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/sip_storage/files/1/2061.jpg	Block	1
66.249.78.254	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4152-he/igf.aspx	Block	1
208.115.113.91	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8348-he	Block	1
66.249.78.167	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
66.249.75.18	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/700-he/bayabashaarchive.aspx	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Unknown HTTP Request Method Söj~ in URL • •ü ú ~wvç•[[#15]]@.. 0	Block	1
148.251.21.227	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-10106-he	Block	1
46.19.86.73	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
66.249.78.242	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6321-he/igf.aspx	Block	1
66.249.78.10	United States	147.237.77.17	mazi.idf.i	Parameter Type Violation PageNum in igf.idf.il/5010-he/igf.aspx	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Illegal Byte Code Character in Query String on • •ü ú ~wvç•[[#15]]@.. 0	Block	1
66.249.69.2	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4142-he/igf.aspx	Block	1
148.251.21.227	Germany	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on igf.idf.il/14-8334-he	Block	1
79.183.62.23	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
66.249.78.167	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/	Block	1
66.249.75.160	United States	147.237.77.17	mazi.idf.i	Parameter Type Violation Back in igf.idf.il/6051-he/igf.aspx	Block	1
148.251.21.227	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/4070-11595-he/.aspx	Block	1