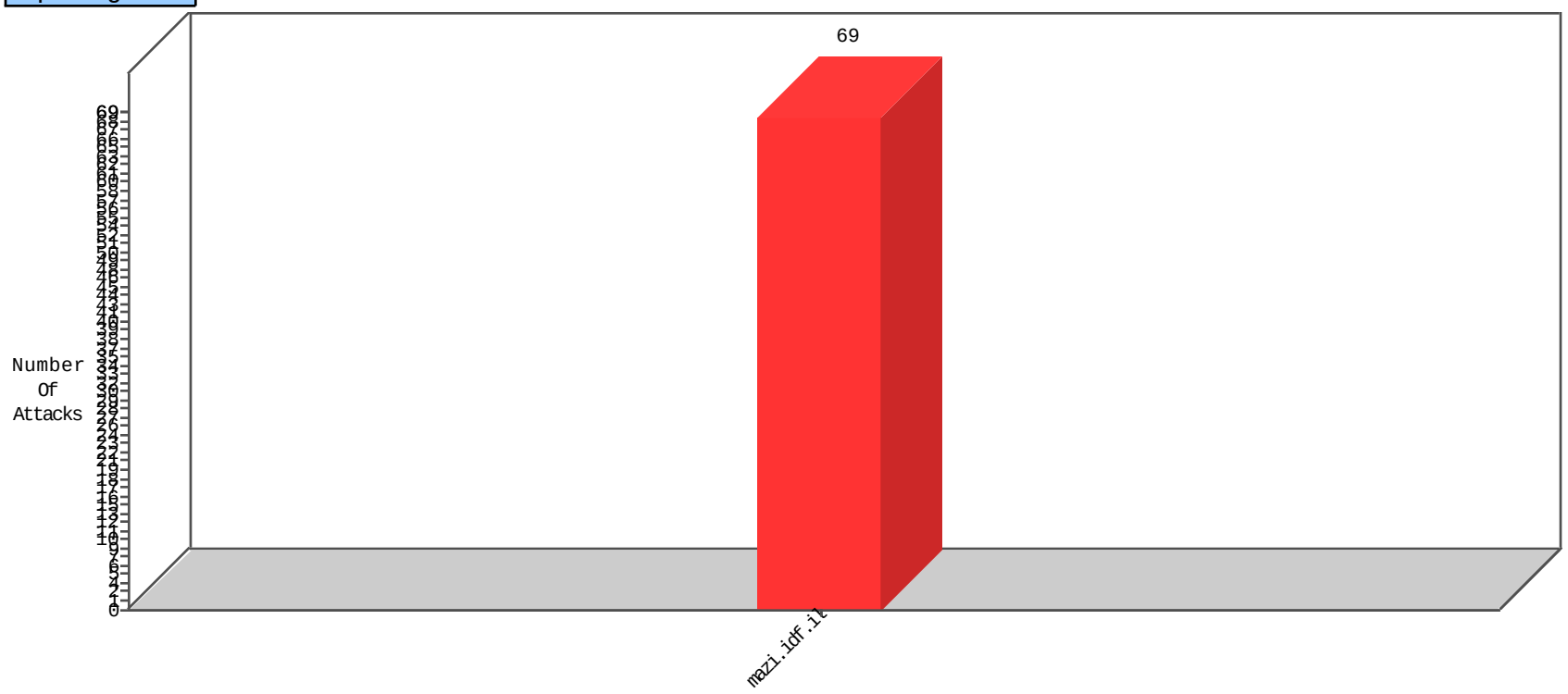
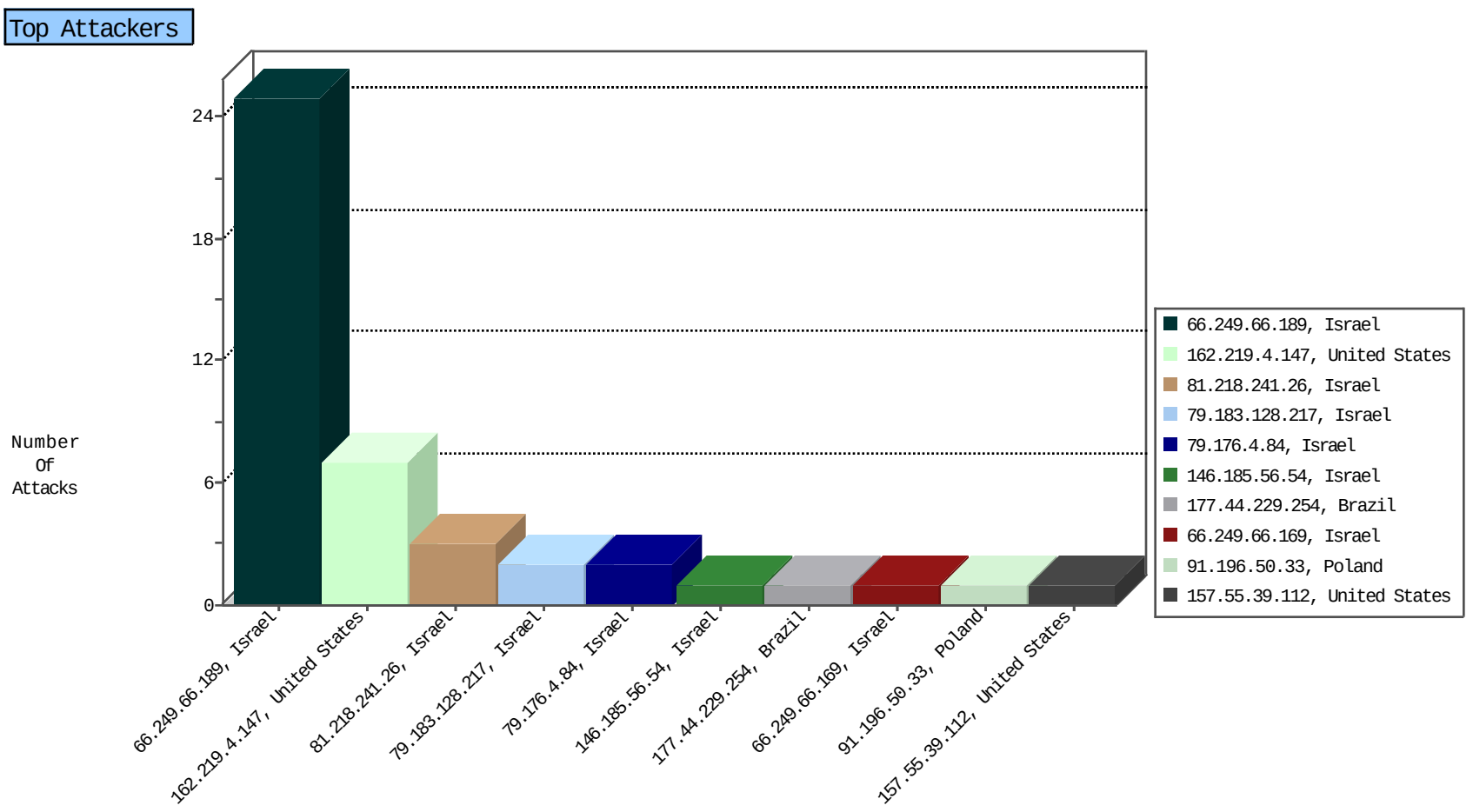
02-16-2016 to 02-17-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



02-16-2016 to 02-17-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.66.189	Israel	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	25
107.150.60.76	United States	147.237.77.17	mazi.idf.il	block-sp-traf1	drop	BBL-Frankfurt	1
173.208.206.203	United States	147.237.77.17	mazi.idf.il	block-sp-traf1	drop	BBL-Frankfurt	1

02-16-2016 to 02-17-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
162.219.4.147	United States	147.237.77.17	mazi.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
188.165.15.236	France	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1
51.255.36.84	United Kingdom	147.237.77.17	mazi.idf.il	C106: HTTP: majestic bot	Block	1
151.80.31.116	Italy	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-16-2016 to 02-17-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
80.83.135.131	Georgia	147.237.77.17	mazi.idf.i	ET SCAN Potential SSH Scan	1
162.219.4.147	United States	147.237.77.17	mazi.idf.i	SERVER-WEBAPP admin.php access	1
177.44.229.254	Brazil	147.237.77.17	mazi.idf.i	ET SCAN Potential SSH Scan	1
5.166.236.157	Russian Federation	147.237.77.17	mazi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
111.37.249.180	China	147.237.77.17	mazi.idf.i	ET SCAN Potential SSH Scan	1
172.4.68.71	United States	147.237.77.17	mazi.idf.i	Tehila - Perl LWP with fake user agent	1
185.130.5.179		147.237.77.17	mazi.idf.i	ET SCAN Potential SSH Scan	1

02-16-2016 to 02-17-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
37.26.148.250	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1029
37.26.148.250	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	583
212.76.127.10	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	81
87.79.69.115	Germany	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	36
87.79.69.115	Germany	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	36
46.19.85.139	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	36
87.79.69.115	Germany	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	36
46.19.85.139	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
87.79.69.115	Germany	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
46.19.85.149	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	25
46.19.85.149	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
37.26.148.250	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence		monitor	20
89.138.63.209	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
37.26.149.241	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
109.64.39.60	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
89.138.63.209	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
212.76.127.111	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
46.19.85.203	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.39	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
72.10.168.87	Canada	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
195.239.16.40	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
37.26.149.241	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
72.10.168.87	Canada	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
195.239.16.53	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
46.117.64.6	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.39	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	9
37.26.148.250	Israel	147.237.77.17	mazi.idf.i	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	9
202.29.239.187	Thailand	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	7
109.65.203.63	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
80.130.105.43	Germany	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.241	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	4
79.176.4.84	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.46.38.220	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
82.166.84.165	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
46.117.64.6	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
185.3.147.223	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
82.166.84.165	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.36.204	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	4
86.25.51.239	United Kingdom	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.128	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
84.95.198.36	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	4
77.127.245.214	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.165.73	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
41.254.8.151	Libyan Arab Jamahiriya	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
14.201.20.180	Australia	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.117.65.199	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.87	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.62	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
87.69.128.8	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
37.46.38.186	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1

02-16-2016 to 02-17-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
81.218.241.26	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 81.218.241.26	Block	3
79.176.4.84	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/images/transvideocounter.gif	Block	2
162.219.4.147	United States	147.237.77.17	mazi.idf.i	PHP Attempt	Block	2
157.55.39.112	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8333-he	Block	1
84.228.245.71	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5676-7827-he/ifg.aspx	Block	1
66.249.66.169	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
162.219.4.147	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/wp-login.php	Block	1
146.185.56.54	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
79.183.128.217	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 79.183.128.217	Block	1
208.115.113.82	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/14-10106-he	Block	1
162.219.4.147	United States	147.237.77.17	mazi.idf.i	Admin Blocking	Block	1
91.196.50.33	Poland	147.237.77.17	mazi.idf.i	Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php	Block	1
68.180.229.218	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/14-8335-he	Block	1
169.229.3.91	United States	147.237.77.17	mazi.idf.i	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
147.234.241.18	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
80.246.130.95	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master$ucHeader$ucSearchControl$txtSearch in www.mazi.idf.il/14-he/igf.aspx	Block	1
46.117.17.48	Israel	147.237.77.17	mazi.idf.i	Parameter Type Violation Master$ucHeader$ucSearchControl$txtSearch in www.mazi.idf.il/165-he/igf.aspx	Block	1
212.179.21.194	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
162.219.4.147	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 162.219.4.147	Block	1
91.200.12.138	Ukraine	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/5479-he/igf.aspx/trackback/	Block	1
195.154.146.225	France	147.237.77.17	mazi.idf.i	Illegal HTTP Version HTTP/	Block	1
157.55.39.95	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8338-he	Block	1
54.172.21.120	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
212.199.57.200	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/7/1087.jpg	Block	1
95.86.118.117	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
79.183.128.217	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
208.115.111.75	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/templates/shared/usercontrols/vodchannel/	Block	1

02-16-2016 to 02-17-2016