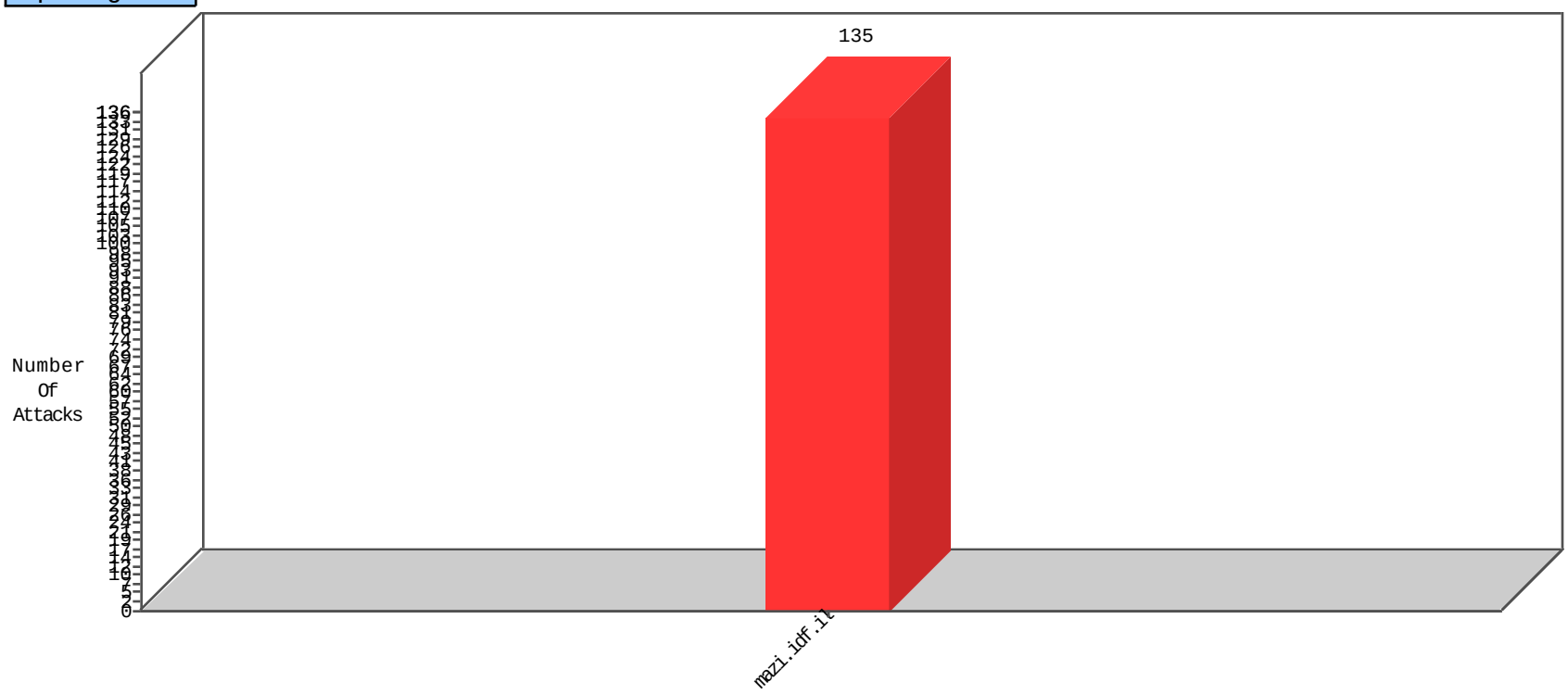
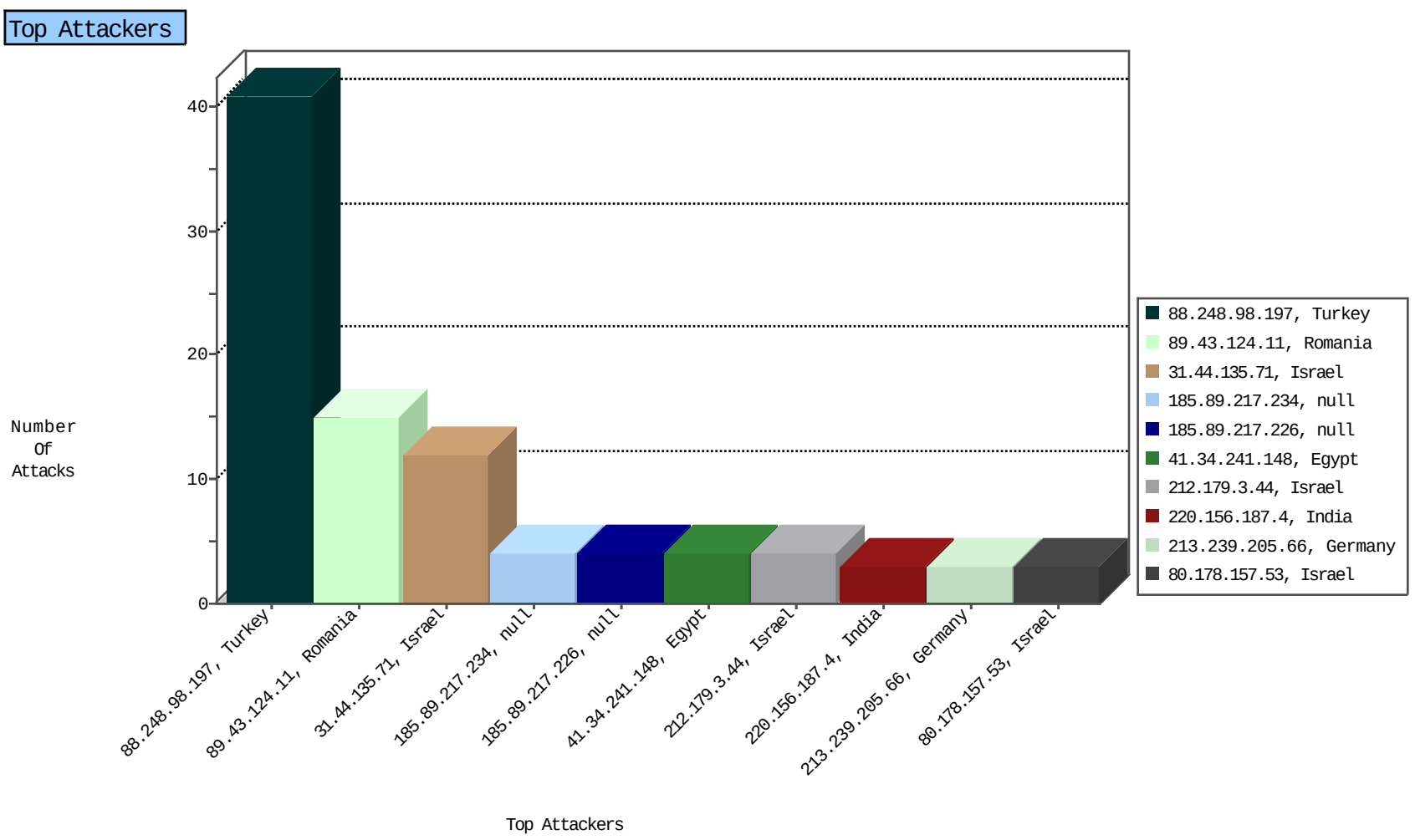
02-11-2016 to 02-12-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



02-11-2016 to 02-12-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.66.134	Israel	147.237.77.17	mazi.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	1

02-11-2016 to 02-12-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
88.248.98.197	Turkey	147.237.77.17	mazi.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	41
220.156.187.4	India	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	3
188.165.15.196	France	147.237.77.17	mazi.idf.il	C228: HTTP: AhrefBot crawler	Block	1
195.10.212.190	Netherlands	147.237.77.17	mazi.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
213.239.205.66	Germany	147.237.77.17	mazi.idf.il	0543: HTTP: php.cgi Access	Block	1
155.94.254.143	United States	147.237.77.17	mazi.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1

02-11-2016 to 02-12-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
5.143.76.26	Russian Federation	147.237.77.17	mazi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
198.12.82.58	United States	147.237.77.17	mazi.idf.i	ET SCAN NMAP -sS window 1024	1
59.45.79.117	China	147.237.77.17	mazi.idf.i	ET SCAN Potential SSH Scan	1

02-11-2016 to 02-12-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
79.127.43.168	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	432
79.127.43.168	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	248
62.219.232.131	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	81
208.115.111.75	United States	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	40
212.76.127.111	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	36
46.19.85.191	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	36
80.178.157.42	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	36
46.19.85.191	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
147.236.34.10	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
212.76.127.219	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	18
37.26.148.131	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
185.89.217.234		147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
185.89.217.226		147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
46.19.85.186	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
195.239.16.53	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
37.26.146.216	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	9
79.178.53.96	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
37.26.146.216	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	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
91.200.12.106	Ukraine	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	8
46.19.85.106	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7
77.127.101.139	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
109.64.237.222	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
185.89.217.229		147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
91.200.12.141	Ukraine	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	4
46.19.85.107	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.18.86	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.180.110.138	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
185.89.217.235		147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
181.170.187.47	Argentina	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.204	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
185.89.217.231		147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
79.182.150.175	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.159	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
212.235.77.210	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
84.109.243.65	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	4
2.52.136.8	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
185.3.144.117	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.144.11	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
2.54.22.203	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
80.82.64.68	Netherlands	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	2
185.89.217.230		147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
2.54.50.87	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
147.236.34.24	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.143.12	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
31.210.188.95	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
183.60.243.189	China	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	1
73.22.239.44	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
147.235.8.77	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
213.57.165.71	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1

02-11-2016 to 02-12-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
31.44.135.71	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	12
89.43.124.11	Romania	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	7
89.43.124.11	Romania	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 89.43.124.11	Block	6
80.178.157.53	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	3
79.183.5.10	Israel	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/templates/newslist/undefined	Block	2
17.138.55.108	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 17.138.55.108	Block	2
41.34.241.148	Egypt	147.237.77.17	mazi.idf.i	PHP Attempt	Block	2
212.179.3.44	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	2
213.239.205.66	Germany	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 213.239.205.66	Block	2
109.65.43.138	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
85.65.202.64	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
46.19.85.60	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
212.179.3.44	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/xmlrpc.php	Block	1
149.78.46.68	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
89.43.124.11	Romania	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/phpmoadmin/moadmin.php	Block	1
41.34.241.148	Egypt	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 41.34.241.148	Block	1
208.115.113.91	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4070-11595-he/×ž×—×œ×§×ª ×ª×›× ×•× ×•×‘×¨×§×¨×”.aspx	Block	1
109.253.206.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files	Block	1
89.43.124.11	Romania	147.237.77.17	mazi.idf.i	Admin Blocking	Block	1
65.55.212.95	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
212.179.3.44	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/xmlrpc.php	Block	1
157.55.39.222	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
94.199.151.22	United Kingdom	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
208.115.113.91	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/Ù…Ù^Ù,Ø¹	Block	1
131.253.24.128	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/templates/newslist/undefined	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8335-he	Block	1
212.235.77.210	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
17.138.55.108	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to igf.idf.il/shared/usercontrols/vodchannel/	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
95.86.95.98	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to m.mazi.idf.il/7322-11795-he/mazi.aspx&sa=u&ved=0ahukewju79qoo_dkahwffw8khqb9apcqfggymau&sig2=uo-slmq-ajhpeuzm1j3evw&usg=afqjcngb9i08tw3fbb4lqxjmi_tdvhcb7w	Block	1
85.65.202.64	Israel	147.237.77.17	mazi.idf.i	Distributed PHP Attempt	Block	1
41.34.241.148	Egypt	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
149.78.46.68	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
79.143.180.15	Germany	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/6367-he/mailto:igf@idf.gov.il	Block	1
185.89.217.232		147.237.77.17	mazi.idf.i	Suspicious Response Code	Block	1

02-11-2016 to 02-12-2016