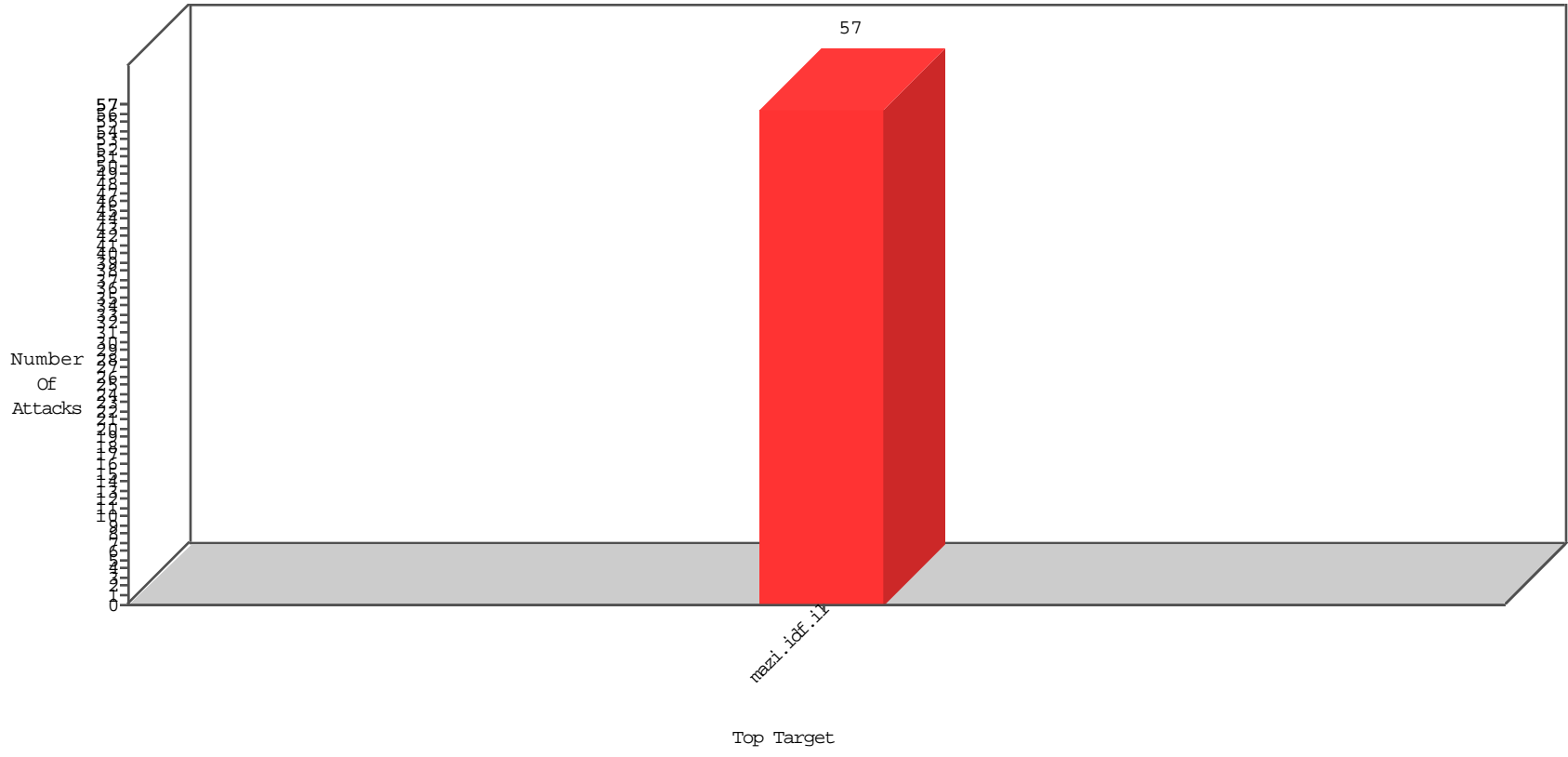


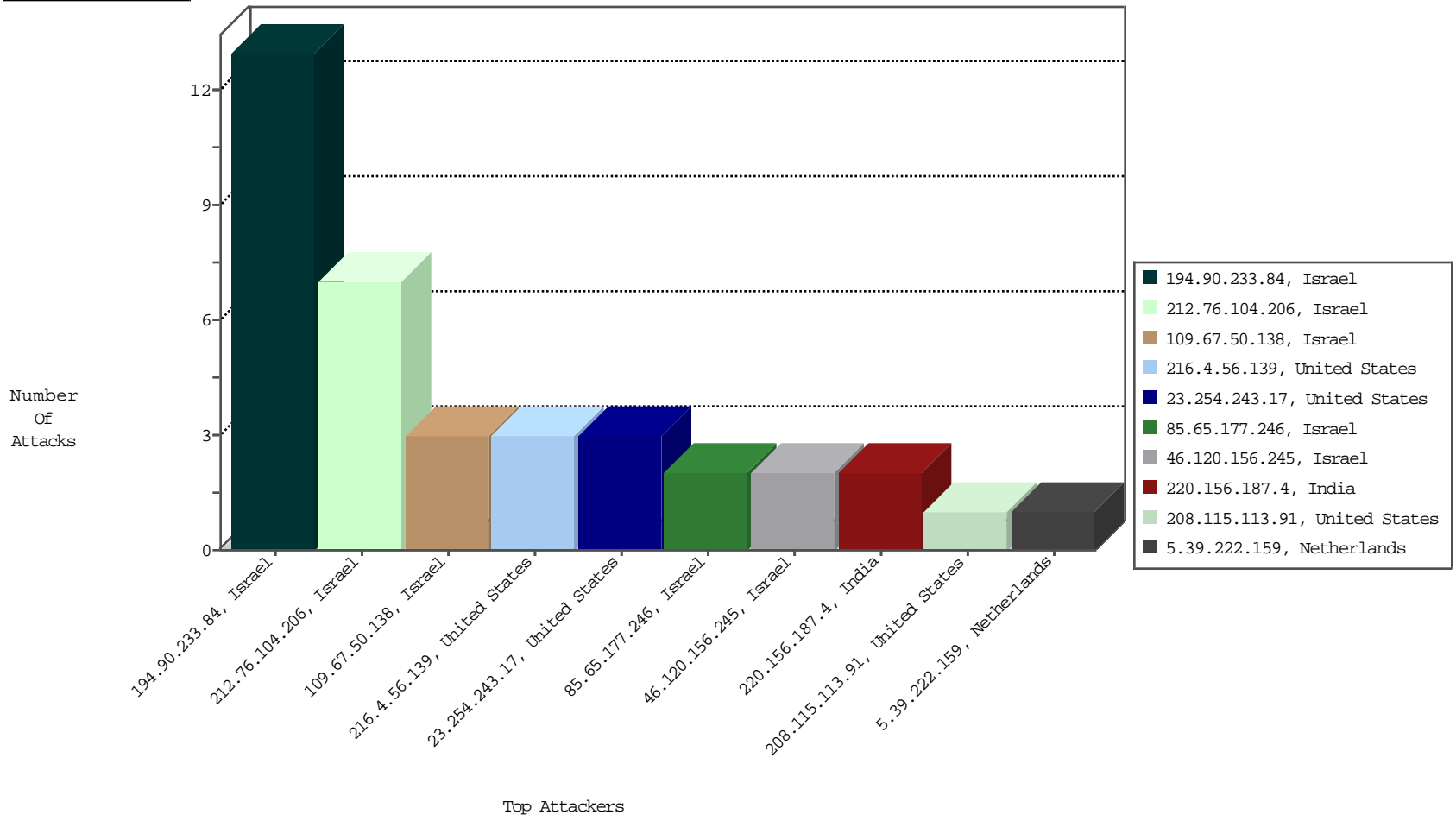
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



02-09-2016 to 02-10-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
109.67.50.138	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	3
142.54.160.214	United States	147.237.77.17	mazi.idf.il	block-sp-trafl	drop	BBL-Frankfurt	1

02-09-2016 to 02-10-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
220.156.187.4	India	147.237.77.17	mazi.idf.in	C228: HTTP: AhrefBot crawler	Block	2
52.33.227.96	United States	147.237.77.17	mazi.idf.in	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
59.45.79.117	China	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1
93.173.250.234	Israel	147.237.77.17	mazi.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
212.47.237.95	France	147.237.77.17	mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.117.208.243		147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
194.1.238.234	Russian Federation	147.237.77.17	mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
84.94.198.122	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	81
84.94.198.122	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	73
46.19.85.43	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	50
81.218.173.8	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid sequence number	monitor	48
80.178.157.42	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	36
46.19.85.7	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	36
212.76.127.10	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	27
46.19.85.43	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	25
212.76.127.44	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	18
46.19.85.231	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
46.19.86.107	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
84.111.50.184	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.231	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	9
212.76.127.219	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	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
46.19.86.107	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	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
2.52.56.207	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.120.156.245	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.102.195.86	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.146.138	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence		monitor	4
64.5.53.237	United States	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
212.76.127.111	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
79.127.43.185	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.170	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
79.127.43.185	Iran, Islamic Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.146.138	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence		alert	4
94.230.86.255	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
213.8.118.60	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
79.176.57.1	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
23.254.243.17	United States	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
2.54.179.183	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
185.3.147.216	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.16.131	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
37.26.147.210	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
2.54.134.138	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
109.184.96.102	Russian Federation	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.81.216	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
149.88.34.112	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
46.120.98.72	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
109.226.28.132	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
216.243.31.2	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.65.124.154	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
46.19.85.230	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
191.144.52.48	Colombia	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
46.19.85.4	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
77.127.127.71	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.13.13.11	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
109.253.158.25	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.117.72.15	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1

02-09-2016 to 02-10-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
194.90.233.84	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 194.90.233.84	Block	10
212.76.104.206	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	5
194.90.233.84	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	3
216.4.56.139	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	3
23.254.243.17	United States	147.237.77.17	mazi.idf.i	Suspicious Response Code	Block	3
46.120.156.245	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/4070-11595-he/xžx-xøxšxª xªx>x x•xŸ x•x'xšx"x".aspx	Block	2
212.76.104.206	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 212.76.104.206	Block	2
95.86.87.32	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/3697-10473-he/igf.aspx&sa=u&ved=0ahukewjphnhsquvkahwme5okhssubkgqfggtmam&usg=afqjncneucm6t8xvjlcvcj-rihnxjeiw4iq	Block	1
66.249.81.216	Israel	147.237.77.17	mazi.idf.i	URL is Above Root Directory m.mazi.idf.il/./images/body.jpg	Block	1
5.29.58.226	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
85.65.177.246	Israel	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
213.8.118.60	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
95.175.35.73	Israel	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 95.175.35.73	Block	1
66.249.81.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/favicon.ico	Block	1
5.39.222.159	Netherlands	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/rom-0	Block	1
208.115.113.91	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8330-he	Block	1
85.65.177.246	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/xmlrpc.php	Block	1
66.249.66.173	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
173.252.75.118	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/6/5826.jpg&imgrefurl=	Block	1
66.249.81.254	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
87.69.196.147	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
66.249.78.242	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
79.176.57.1	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
46.19.86.200	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1

02-09-2016 to 02-10-2016