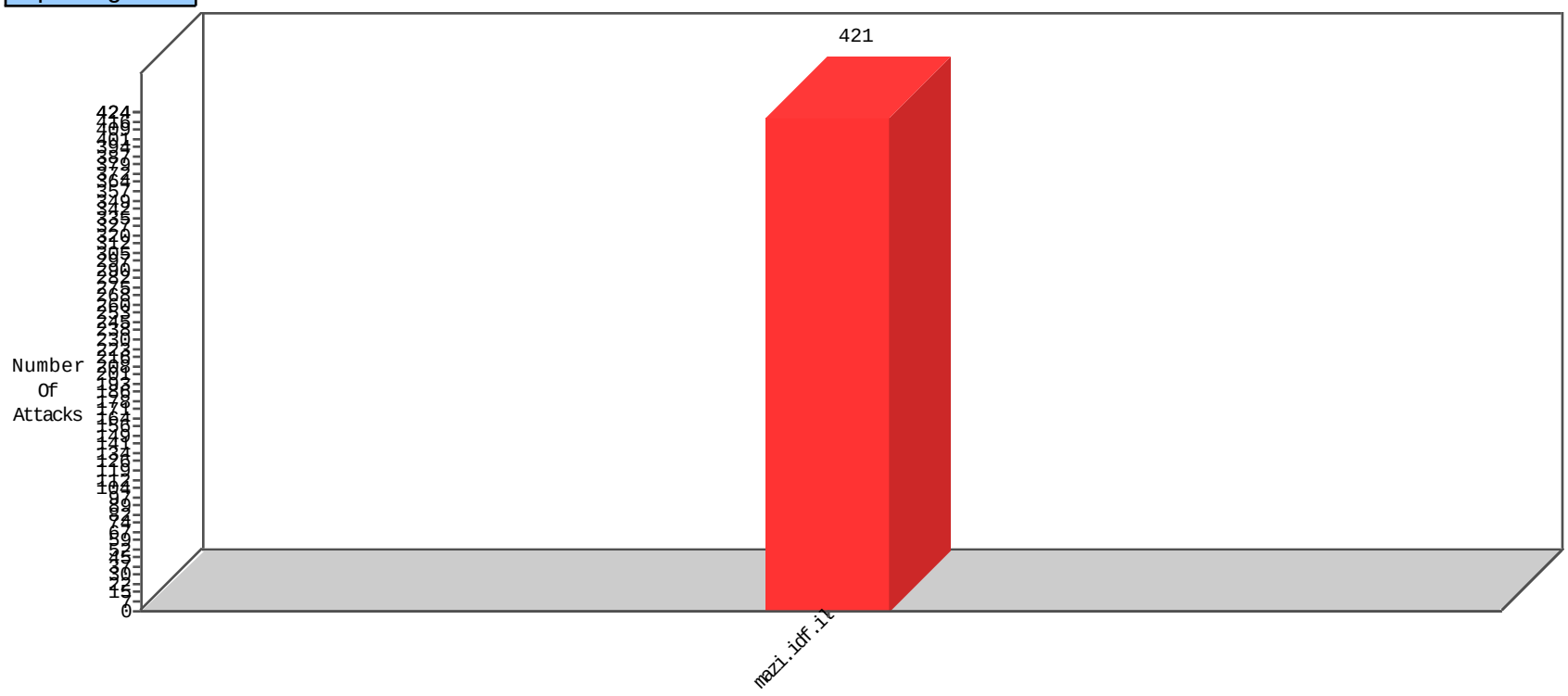
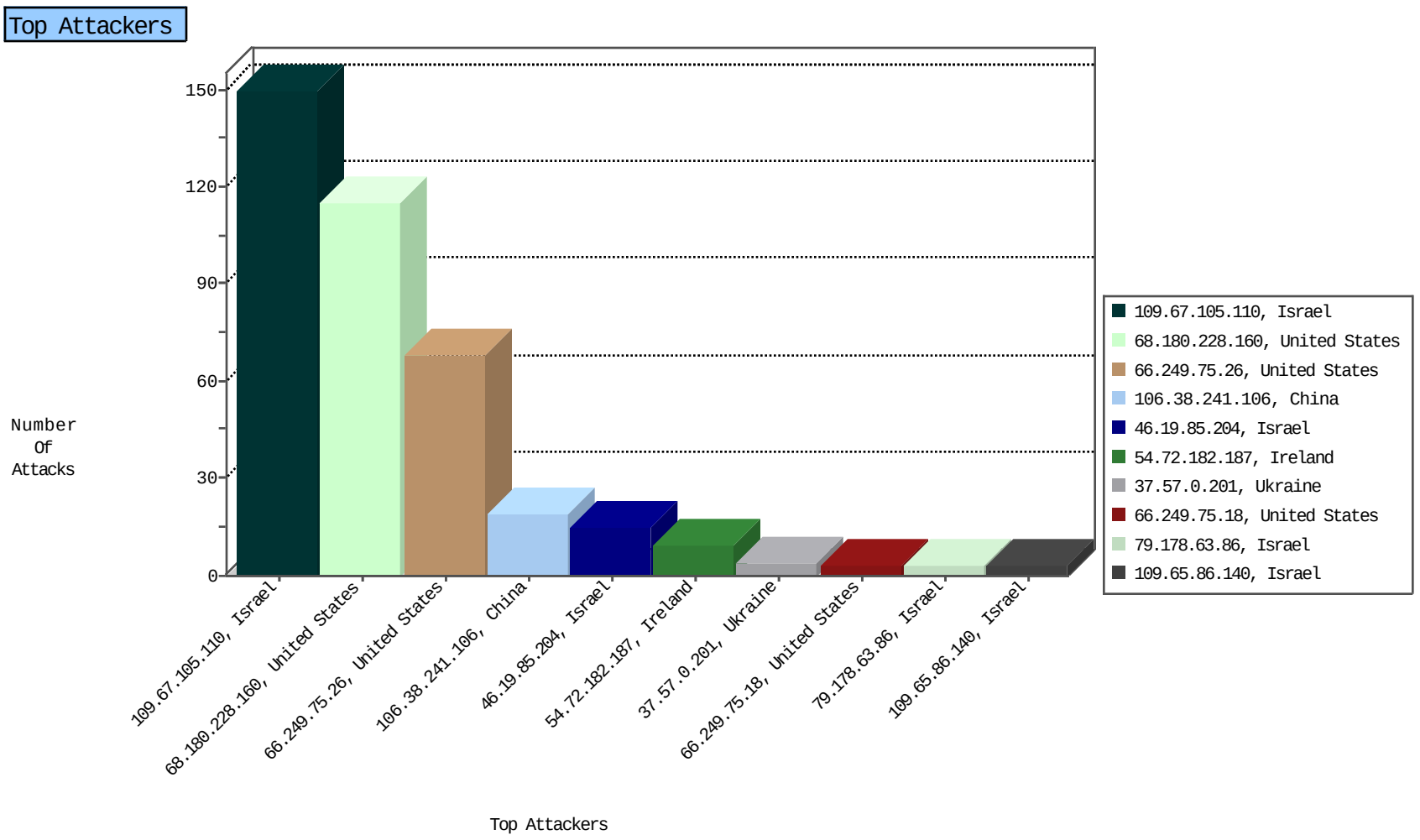
03-04-2016 to 03-05-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



03-04-2016 to 03-05-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
54.72.182.187	Ireland	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	9
109.65.86.140	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	3
184.105.247.228	United States	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
204.42.253.2	United States	147.237.77.17	mazi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
213.238.176.44	Turkey	147.237.77.17	mazi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
71.6.167.142	United States	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
89.248.160.138	Netherlands	147.237.77.17	mazi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1

03-04-2016 to 03-05-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
109.67.105.110	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	150
68.180.228.160	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	114
106.38.241.106	China	147.237.77.17	mazi.idf.il	C10000071: HTTP: User Agent Sogou+web+spider	Block	19
46.19.85.204	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
85.64.149.183	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
144.76.8.132	Germany	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
157.55.12.92	United States	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.17.177.214	Kazakstan	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.178.154.141	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
136.243.103.92	Germany	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
188.165.15.196	France	147.237.77.17	mazi.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
37.57.0.201	Ukraine	147.237.77.17	mazi.idf.il	C1000016: HTTP: administrator in URI	Block	1

03-04-2016 to 03-05-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.75.26	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	68
66.249.75.18	United States	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sA (2)	2
128.199.41.249	Singapore	147.237.77.17	mazi.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
82.118.233.119	Bulgaria	147.237.77.17	mazi.idf.il	ET SCAN Potential SSH Scan	1

03-04-2016 to 03-05-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
31.168.16.60	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	69
46.19.86.92	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
46.19.85.191	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	49
46.19.85.191	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	49
192.243.55.130	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
192.243.55.130	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
192.243.55.131	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
192.243.55.129	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
181.112.204.130	Ecuador	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
192.243.55.129	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
181.112.204.130	Ecuador	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
37.26.148.207	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.19.86.92	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
192.243.55.138	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
212.125.69.106	United Kingdom	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
192.243.55.135	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
192.243.55.135	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
192.243.55.132	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.137	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.135	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.131	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
192.243.55.130	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
192.243.55.138	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
37.142.74.36	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
192.243.55.135	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	12
192.243.55.130	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	12
192.243.55.130	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	12
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.133	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.137	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
192.243.55.129	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
192.243.55.138	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
192.243.55.129	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
5.29.165.192	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
87.69.174.31	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
5.29.165.192	Israel	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
192.243.55.135	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
192.243.55.137	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.129	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence		monitor	8
192.243.55.138	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
192.243.55.134	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
192.243.55.131	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
192.243.55.133	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.131	Dominica	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.136	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.133	Dominica	147.237.77.17	mazi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
85.130.170.218	Israel	147.237.77.17	mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6

03-04-2016 to 03-05-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
79.178.63.86	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	3
192.243.55.138	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8338-he	Block	1
149.88.200.21	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/571-he/igf.aspx	Block	1
37.57.0.201	Ukraine	147.237.77.17	mazi.idf.i	PHP Attempt	Block	1
192.243.55.130	Dominica	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 192.243.55.130	Block	1
207.46.13.94	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
157.55.39.106	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/robots.txt	Block	1
37.57.0.201	Ukraine	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/wp-login.php	Block	1
192.243.55.135	Dominica	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/14-8348-he	Block	1
87.69.174.31	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
2.54.49.20	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	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
66.249.75.18	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/newsgallery/	Block	1
192.243.55.138	Dominica	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 192.243.55.138	Block	1
104.131.147.112	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5216-he/igf.aspx	Block	1
37.57.0.201	Ukraine	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 37.57.0.201	Block	1
185.112.248.32		147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/450-he.aspx	Block	1

03-04-2016 to 03-05-2016