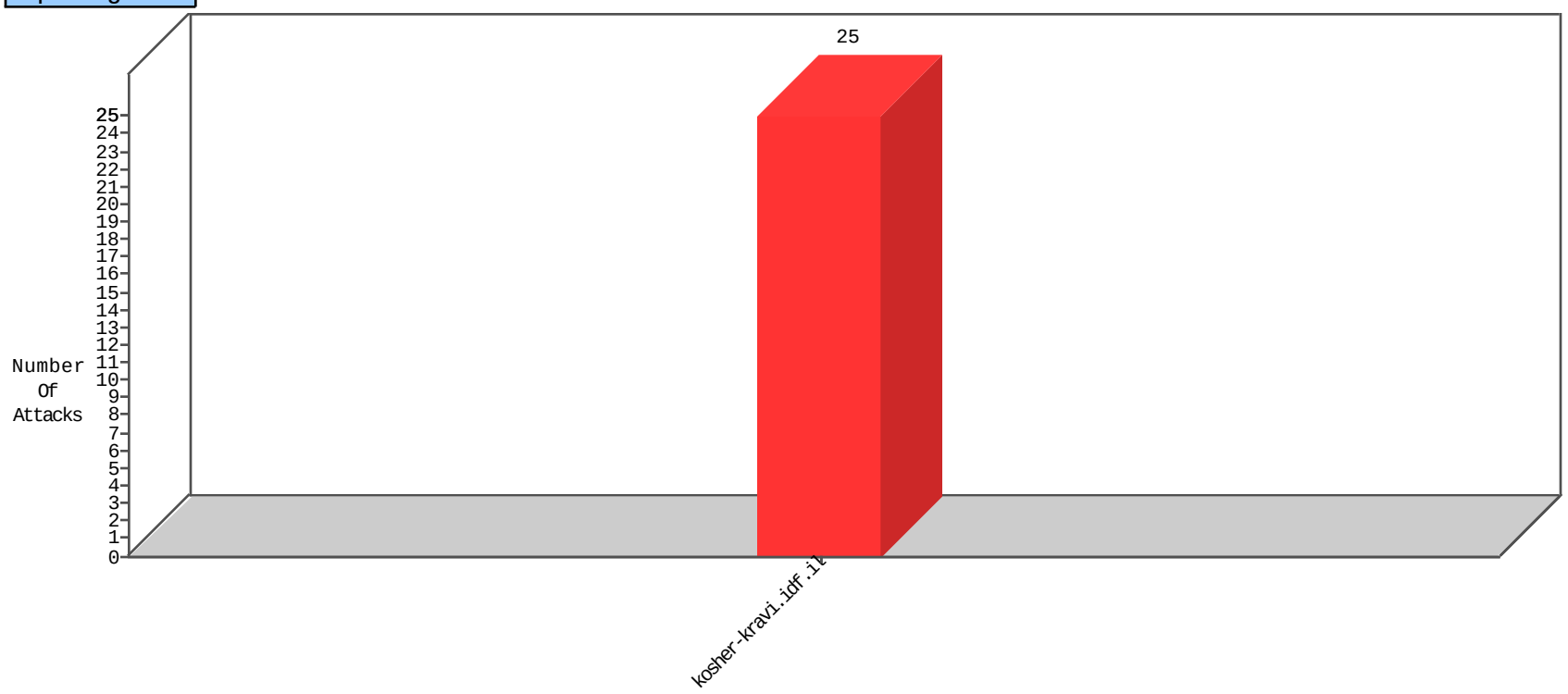
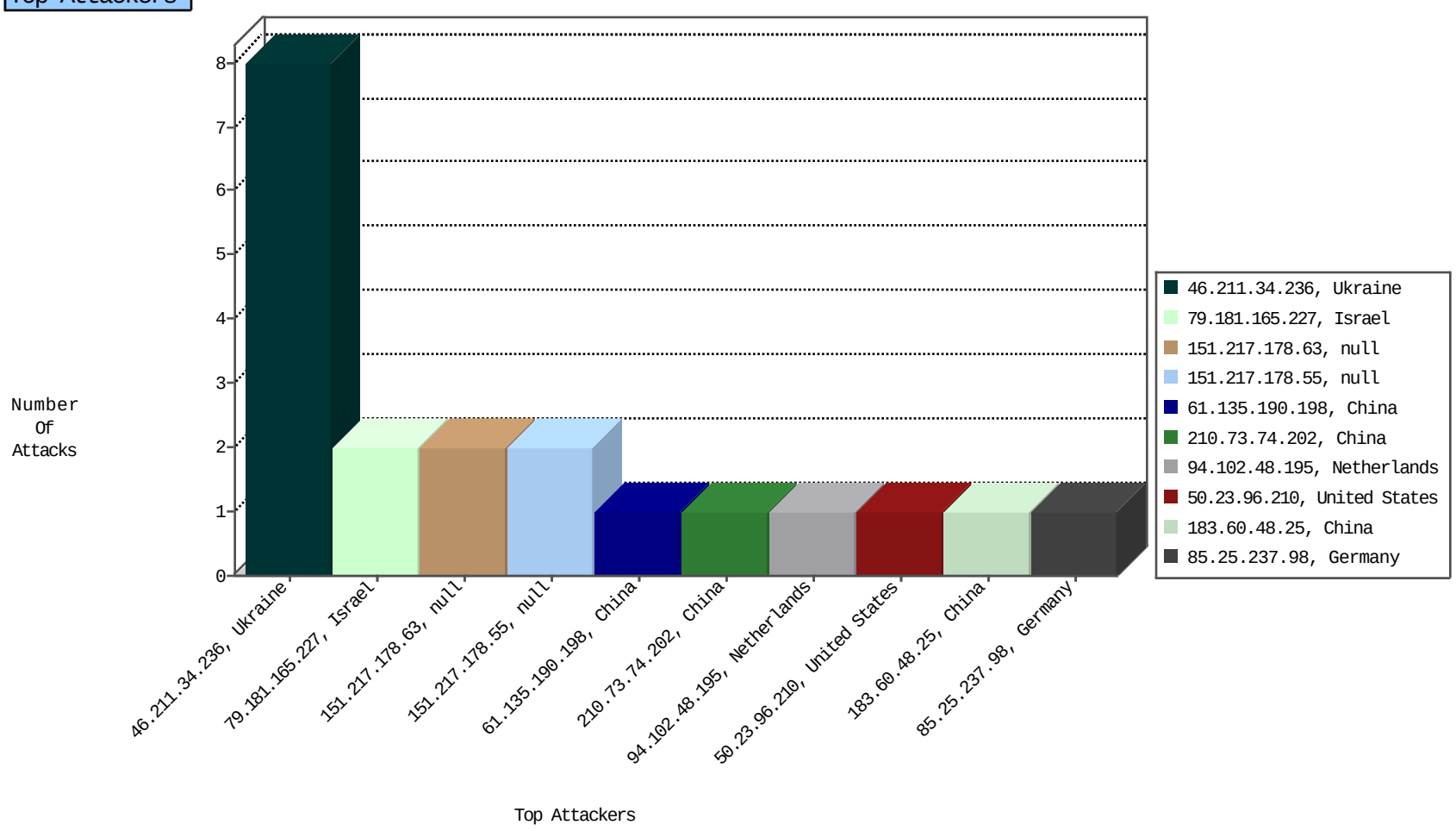
12-28-2015 to 12-29-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-28-2015 to 12-29-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count

12-28-2015 to 12-29-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-28-2015 to 12-29-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
151.217.178.63		147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential VNC Scan 5900-5920	2
151.217.178.55		147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential VNC Scan 5900-5920	2
222.186.34.80	China	147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
46.211.34.236	Ukraine	147.237.0.15	kosher-kravi.idf.i	SERVER-WEBAPP admin.php access	1
94.102.48.195	Netherlands	147.237.0.15	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
183.60.48.25	China	147.237.0.15	kosher-kravi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
212.47.229.34	France	147.237.0.15	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
50.23.96.210	United States	147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
151.217.178.88		147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
210.73.74.202	China	147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1

12-28-2015 to 12-29-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
61.216.2.13	Taiwan	147.237.0.15	kosher-kravi.idf.i	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	9
216.243.31.2	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
128.232.110.28	United Kingdom	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
141.212.122.119	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.218.251.250	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
61.216.2.13	Taiwan	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.228	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.194	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
71.6.216.53	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.90	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.168	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.25.237.98	Germany	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
61.216.2.13	Taiwan	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
210.44.144.110	China	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
151.217.97.185		147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.112	United States	147.237.0.15	kosher-kravi.idf.i	drop	SAM rule	drop	1
74.82.47.28	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.187.114.171	France	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.169	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
101.198.159.31	China	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
151.217.178.93		147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.118	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.30	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
52.28.32.164	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
176.13.9.130	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.193	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
115.231.0.57	China	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
64.125.239.239	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
169.229.3.90	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	alert	1

12-28-2015 to 12-29-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
46.211.34.236	Ukraine	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 46.211.34.236	Block	2
46.211.34.236	Ukraine	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	2
85.25.237.98	Germany	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
61.216.2.13	Taiwan	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 8.8.8.8/404	Block	1
2.54.8.68	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/sip_storage/files/3/1903.pd	Block	1
79.181.165.227	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
46.211.34.236	Ukraine	147.237.0.15	kosher-kravi.idf.il	Admin Blocking	Block	1
46.211.34.236	Ukraine	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/wp-login.php	Block	1
79.181.165.227	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/xmlrpc.php	Block	1
46.211.34.236	Ukraine	147.237.0.15	kosher-kravi.idf.il	Multiple Admin Blocking from 46.211.34.236	Block	1
61.135.190.198	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1

12-28-2015 to 12-29-2015