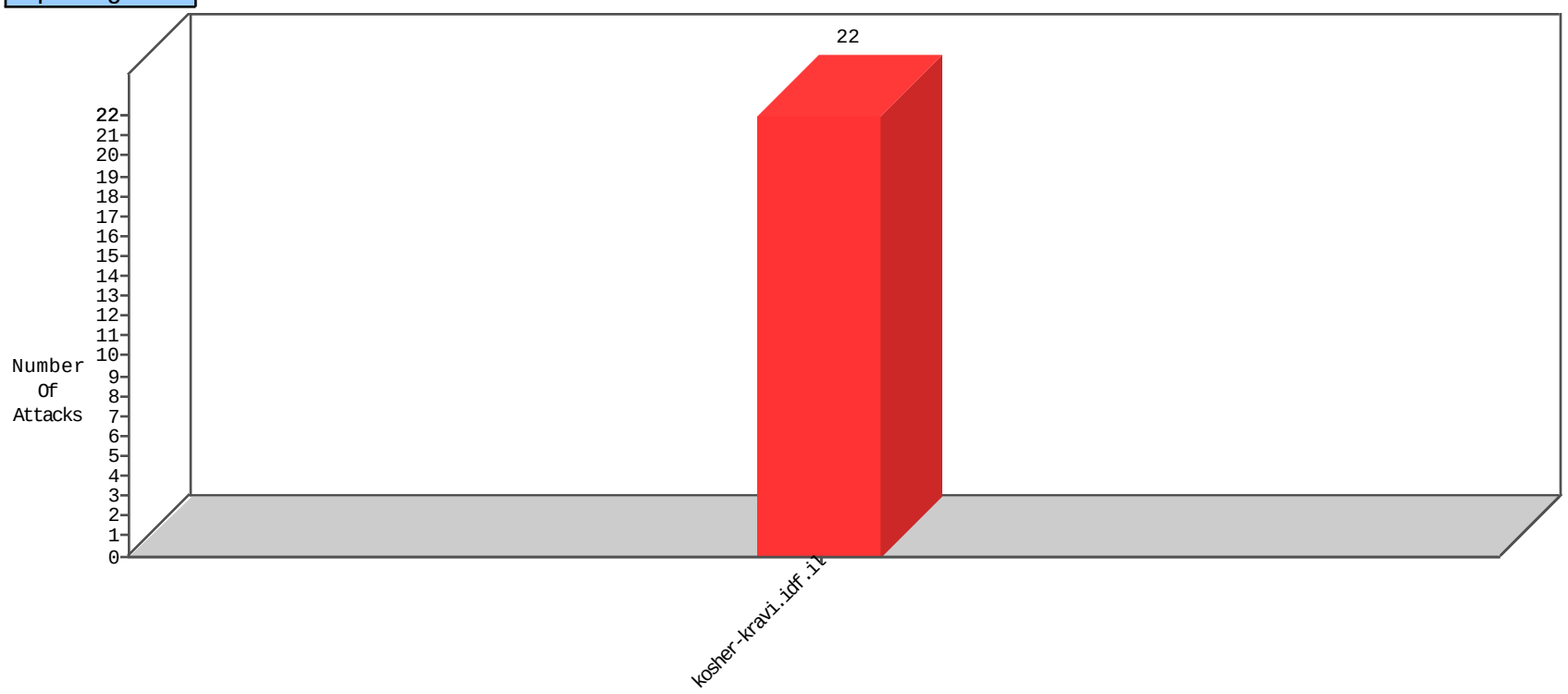
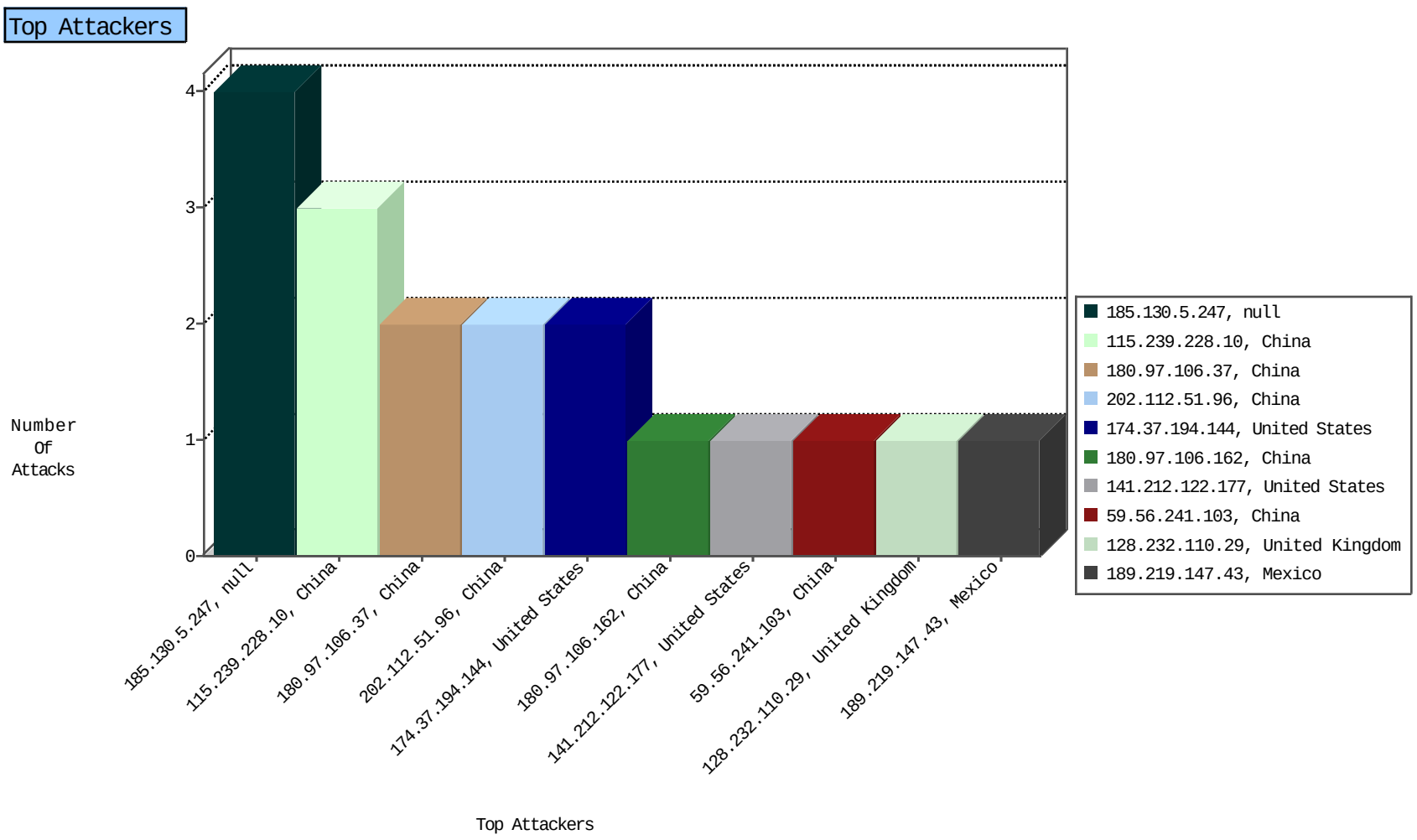
01-15-2016 to 01-16-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-15-2016 to 01-16-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
115.239.228.10	China	147.237.0.15	kosher-kravi.idf.il	Frk_Under_Attack_Con_Http	drop	BBL-Frankfurt	2
180.97.106.162	China	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	drop	BBL-Frankfurt	1
202.112.51.96	China	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	DP-Tehila	1
115.239.228.10	China	147.237.0.15	kosher-kravi.idf.il	Frk_Purple_Con_Limit_Http	drop	BBL-Frankfurt	1

01-15-2016 to 01-16-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
185.130.5.247		147.237.0.15	kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	2
185.130.5.247		147.237.0.15	kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
151.80.31.114	Italy	147.237.0.15	kosher-kravi.idf.il	C228: HTTP: AhrefBot crawler	Block	1

01-15-2016 to 01-16-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
89.248.166.146	Netherlands	147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
149.71.157.125	Italy	147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
174.37.194.144	United States	147.237.0.15	kosher-kravi.idf.i	ET SCAN NMAP -sS window 2048	1
185.130.5.247		147.237.0.15	kosher-kravi.idf.i	ET WEB_SERVER Muieblackcat scanner	1
59.56.241.103	China	147.237.0.15	kosher-kravi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.251.56.171	Ukraine	147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
174.37.194.144	United States	147.237.0.15	kosher-kravi.idf.i	ET SCAN NMAP -f -sS	1
180.97.106.37	China	147.237.0.15	kosher-kravi.idf.i	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

01-15-2016 to 01-16-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
185.130.5.247		147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.195	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
216.243.31.2	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
128.232.110.28	United Kingdom	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
37.26.149.222	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
202.112.51.96	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
174.37.194.144	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
104.45.18.178	United States	147.237.0.15	kosher-kravi.idf.il	Instant Messengers	instant messenger pattern found, application: Skype	monitor	1
64.125.239.179	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.35.62.91	Switzerland	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.185	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
77.127.217.136	Israel	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.151	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
180.76.15.150	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
71.6.165.200	United States	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
141.212.122.186	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.241.222.98	Germany	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
184.105.139.106	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.171	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.10	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.247		147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
84.228.236.56	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
52.28.32.164	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.114	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.172	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.51	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

01-15-2016 to 01-16-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
141.212.122.177	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
180.97.106.37	China	147.237.0.15	kosher-kravi.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
189.219.147.43	Mexico	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
128.232.110.29	United Kingdom	147.237.0.15	kosher-kravi.idf.il	Distributed Unauthorized URL Access on 147.237.0.15/	Block	1
202.112.51.96	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.linkedin.com/	Block	1

01-15-2016 to 01-16-2016