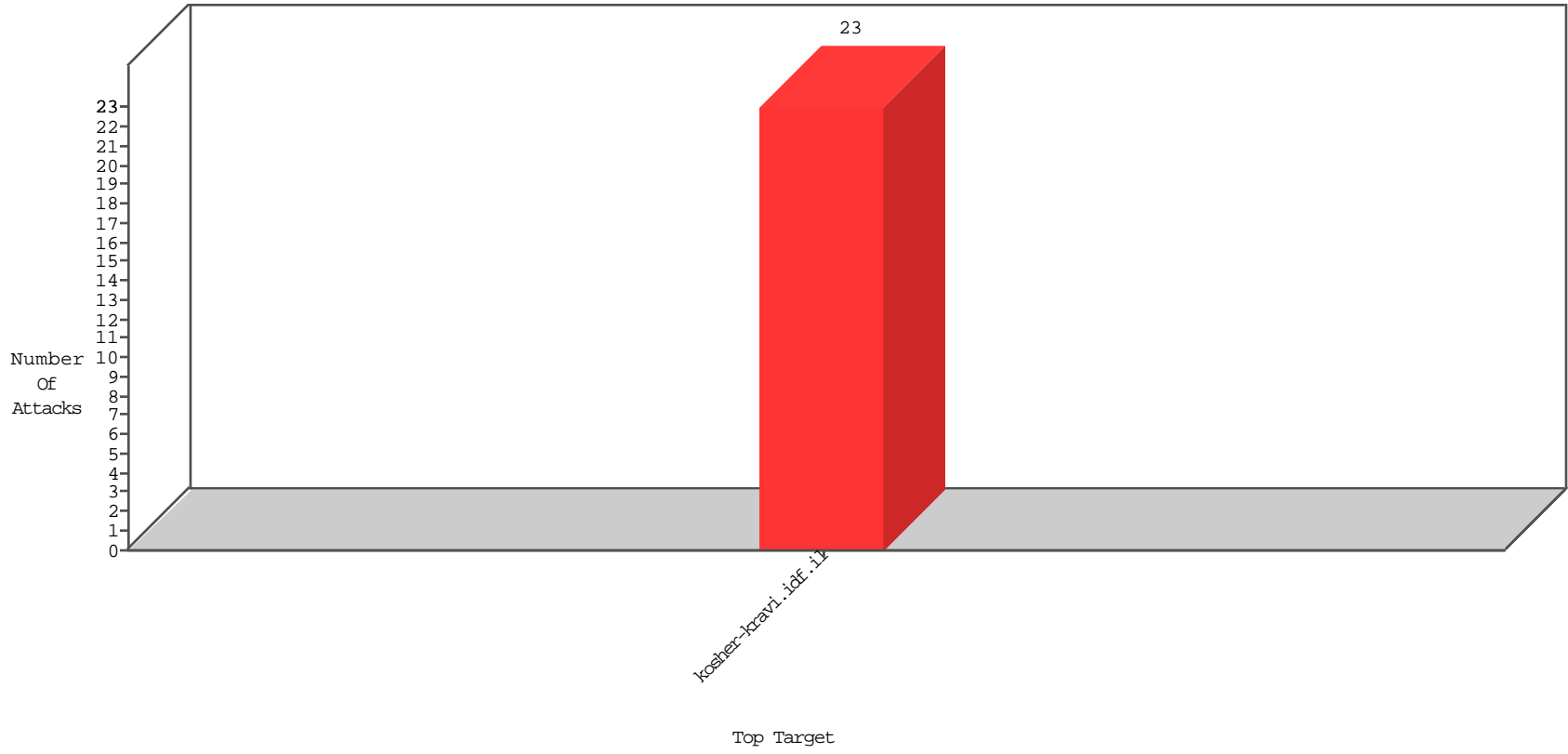


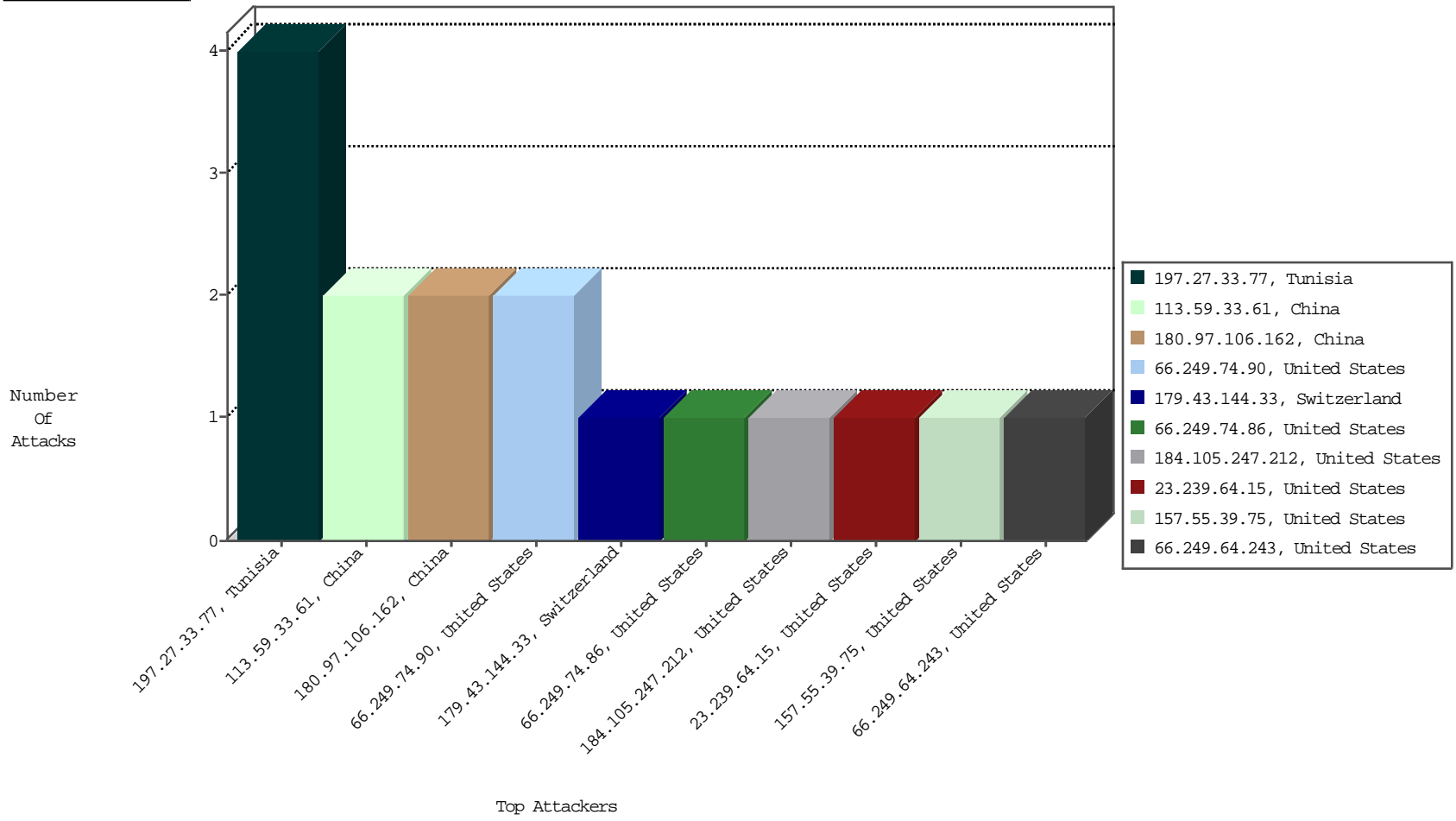
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
23.239.64.15	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
179.43.144.33	Switzerland	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
184.105.139.126	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
184.105.247.212	United States	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	NetV-London	1

02-29-2016 to 03-01-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
66.249.64.10	Israel	147.237.0.15	kosher-kravi.idf.i	12890: TCP: Windows TCP/IP Denial-of-Service Vulnerability (ONLY enable when under DoS attack)	Block	1

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
113.59.33.61	China	147.237.0.15	kosher-kravi.idf.i	ET SCAN NMAP -f -sS	1
122.228.207.118	China	147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
180.210.201.112	Singapore	147.237.0.15	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.15	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
113.59.33.61	China	147.237.0.15	kosher-kravi.idf.i	ET SCAN NMAP -sS window 2048	1
180.97.106.162	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
185.130.5.249		147.237.0.15	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
46.19.86.198	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
46.19.86.198	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.99	Israel	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
216.243.31.2	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.85.40	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
74.82.47.32	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.97.106.36	China	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
141.212.122.148	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.117.167.120	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
159.122.254.235	Netherlands	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
89.248.160.136	Netherlands	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.72	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.149	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
64.125.239.49	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
159.226.95.66	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
91.217.10.157	Ukraine	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.104	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
146.185.239.102	Russian Federation	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
71.6.216.51	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
139.162.40.248	Netherlands	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.117.167.120	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.218.206.118	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
159.122.222.119	Netherlands	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

02-29-2016 to 03-01-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
197.27.33.77	Tunisia	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 197.27.33.77	Block	4
66.249.74.86	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/news/news.in.aspx	Block	1
180.97.106.162	China	147.237.0.15	kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.74.90	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/departmentslobby/departmentslobby.aspx	Block	1
46.19.85.250	Israel	147.237.0.15	kosher-kravi.idf.il	Parameter Type Violation searchText in kosher-kravi.idf.il/1193-he/orchot.aspx	Block	1
66.249.74.90	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/homepage/homepage.aspx	Block	1
66.249.64.243	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/news/news.in.aspx	Block	1
157.55.39.75	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/general/general.aspx	Block	1

02-29-2016 to 03-01-2016