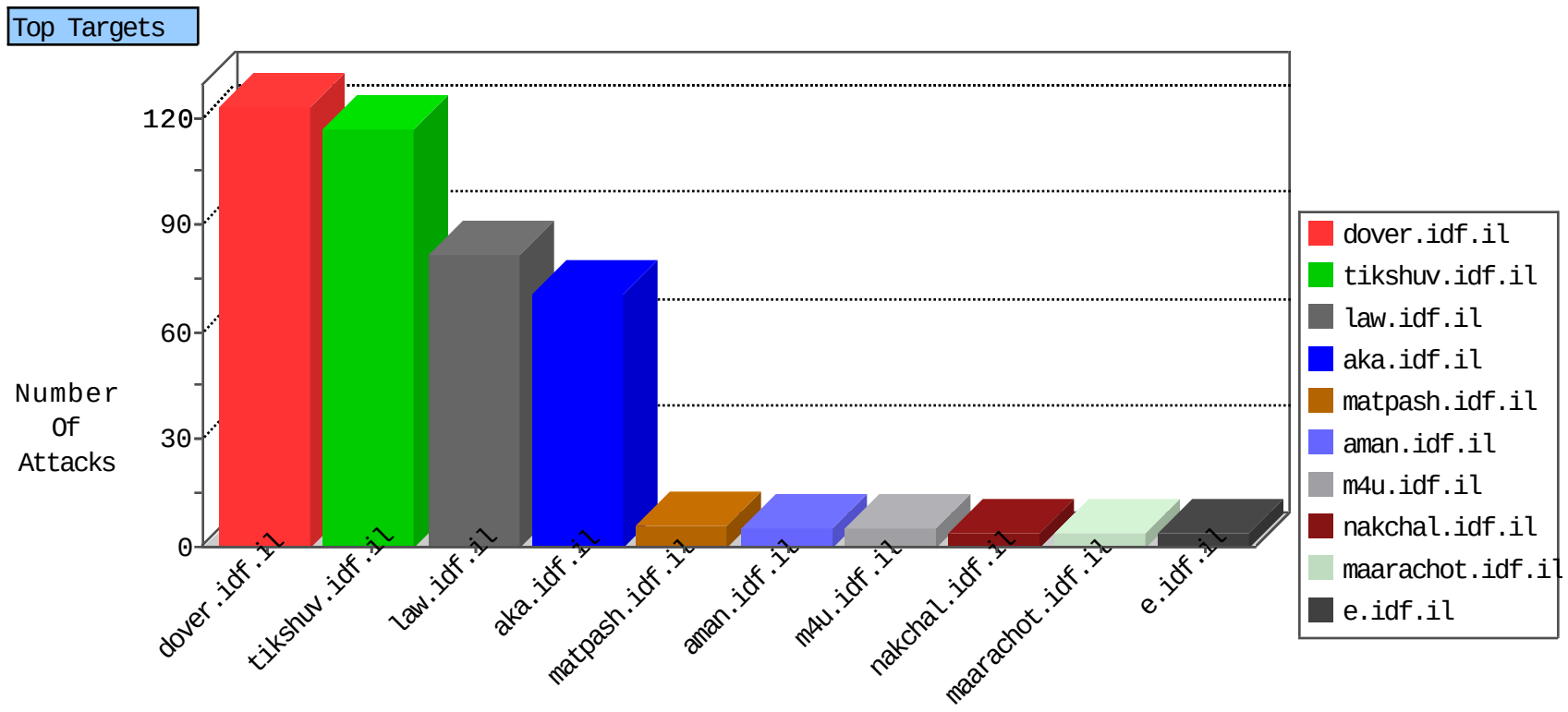
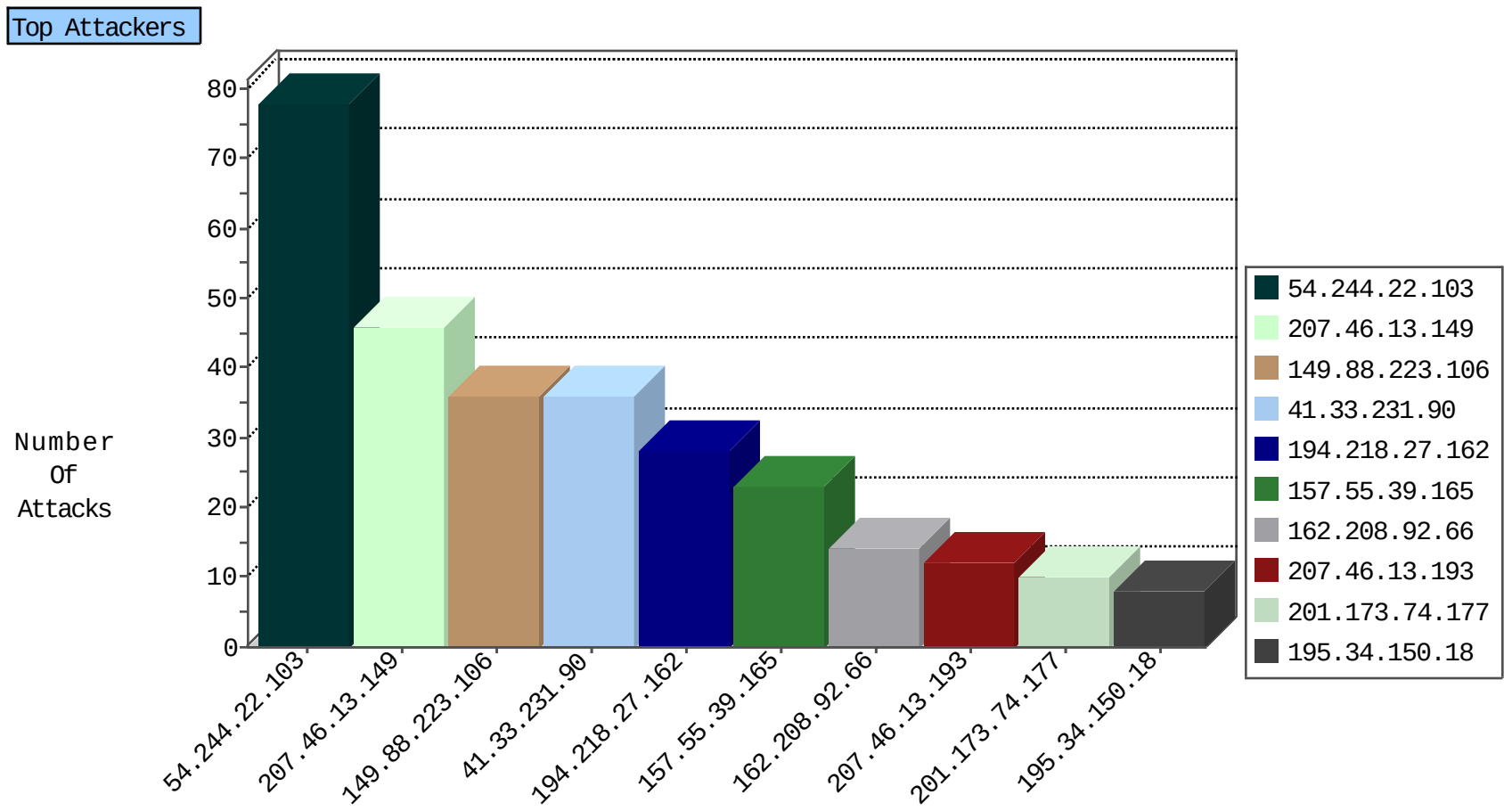
02-23-2016-02:04:00 to 02-23-2016-03:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-23-2016-02:04:00 to 02-23-2016-03:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.10	China	147.237.0.200	m4u.idf.il	Frk_Under_Attack_Con_Http	drop	2
115.239.228.10	China	147.237.0.200	m4u.idf.il	Frk_Purple_Con_Limit_Http	drop	1
115.239.228.10	China	147.237.76.201	e.atal.idf.il	JLM_Purple_Con_Limit_Http	drop	1
173.208.206.206	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1

02-23-2016-02:04:00 to 02-23-2016-03:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.88.223.106	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	36
106.120.173.130	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
157.55.39.97	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
158.69.200.204	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
23.239.85.119	United States	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
40.77.167.71	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

02-23-2016-02:04:00 to 02-23-2016-03:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
98.119.105.221	147.237.8.45	United States	e.eitan.idf.	ET SCAN NMAP -f -sS	1
103.231.125.237	147.237.0.200	India	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.8.45	United States	e.eitan.idf.	ET SCAN NMAP -sS window 2048	1
187.181.35.252	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
98.119.105.221	147.237.8.45	United States	e.eitan.idf.	ET SCAN NMAP -sS window 4096	1

02-23-2016-02:04:00 to 02-23-2016-03:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	75
207.46.13.149	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	46
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
157.55.39.165	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
162.208.92.66	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.46.13.193	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
207.46.13.193	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
207.46.13.19	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.120	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	4
201.173.74.177	Mexico	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
185.27.105.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
40.77.167.98	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
209.52.88.67	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
176.13.8.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
40.77.167.13	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
157.55.39.187	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
207.46.13.107	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
199.30.24.222	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
207.46.13.193	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
201.173.74.177	Mexico	147.237.72.156	aman.idf.il	drop	SAM rule	drop	2
157.55.39.50	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
157.55.2.130	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.29	United Kingdom	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
201.173.74.177	Mexico	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
162.209.124.35	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
62.210.136.217	France	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
128.232.110.29	United Kingdom	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	2
201.173.74.177	Mexico	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
207.46.13.42	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
199.30.24.222	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
66.249.81.196	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.29	United Kingdom	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
72.229.170.241	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
66.249.64.186	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
148.251.13.51	Germany	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1

02-23-2016-02:04:00 to 02-23-2016-03:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-23-2016-02:04:00 to 02-23-2016-03:04:00