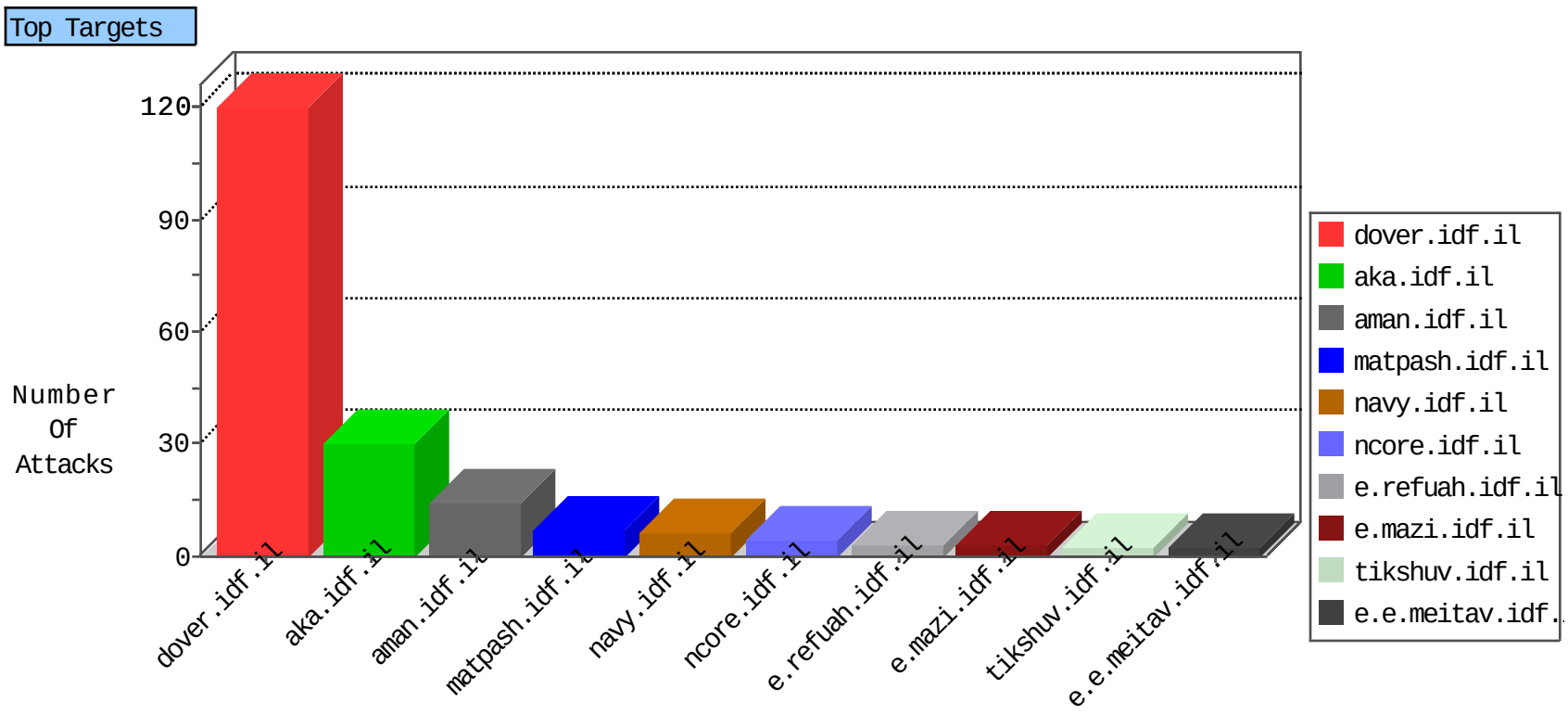
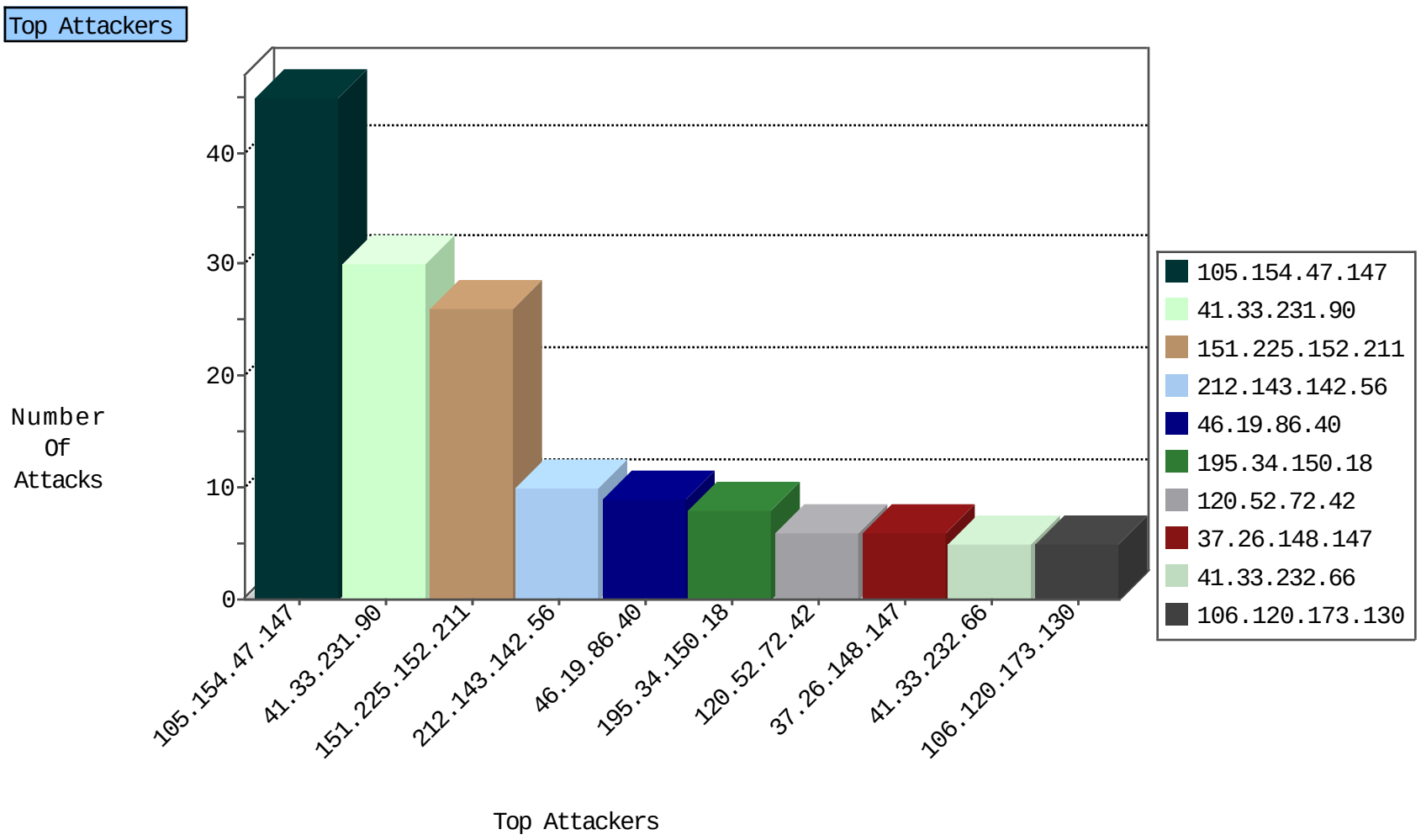
02-23-2016-01:07:05 to 02-23-2016-02:07:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-23-2016-01:07:05 to 02-23-2016-02:07:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
105.154.47.147	Morocco	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
185.130.5.201		147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.201		147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.201		147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
198.20.69.98	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.201		147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

02-23-2016-01:07:05 to 02-23-2016-02:07:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.130	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
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
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
105.154.47.147	Morocco	147.237.77.216	dover.idf.il	16527: TCP: Evaluated Base64 PHP Code	Permit	1

02-23-2016-01:07:05 to 02-23-2016-02:07:05

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
151.225.152.211	147.237.76.177	United Kingdom	ncore.idf.il	ET SCAN Potential SSH Scan	2
151.225.152.211	147.237.77.216	United Kingdom	dover.idf.il	ET SCAN Potential SSH Scan	2
151.225.152.211	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN Potential SSH Scan	1
103.231.125.237	147.237.76.200	India	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 2048	1
151.225.152.211	147.237.76.148	United Kingdom	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
151.225.152.211	147.237.77.227	United Kingdom	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
61.216.84.147	147.237.0.35	Taiwan	akaws.idf.il	ET SCAN Potential SSH Scan	1
151.225.152.211	147.237.76.38	United Kingdom	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
151.225.152.211	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN Potential SSH Scan	1
151.225.152.211	147.237.77.179	United Kingdom	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
151.225.152.211	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN Potential SSH Scan	1
151.225.152.211	147.237.77.121	United Kingdom	e.navy.idf.il	ET SCAN Potential SSH Scan	1
151.225.152.211	147.237.72.14	United Kingdom	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
151.225.152.211	147.237.77.19	United Kingdom	law-forum.idf.il	ET SCAN Potential SSH Scan	1
105.154.47.147	147.237.77.216	Morocco	dover.idf.il	ETPRO WEB_SERVER PHP Possible Open Flash Direct Access to File Upload Directory	1
151.225.152.211	147.237.76.198	United Kingdom	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
105.154.47.147	147.237.77.216	Morocco	dover.idf.il	ET WEB_SERVER HTTP POST Generic eval of base64_decode	1
151.225.152.211	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
151.225.152.211	147.237.76.176	United Kingdom	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
186.235.100.2	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
98.119.105.221	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -f -sS	1
151.225.152.211	147.237.76.44	United Kingdom	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
151.225.152.211	147.237.77.226	United Kingdom	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
61.216.84.147	147.237.0.34	Taiwan	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
151.225.152.211	147.237.76.31	United Kingdom	nakchal.idf.il	ET SCAN Potential SSH Scan	1
151.225.152.211	147.237.77.212	United Kingdom	e.dover.idf.il	ET SCAN Potential SSH Scan	1
151.225.152.211	147.237.72.167	United Kingdom	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
151.225.152.211	147.237.77.176	United Kingdom	matpash.idf.il	ET SCAN Potential SSH Scan	1
151.225.152.211	147.237.72.156	United Kingdom	aman.idf.il	ET SCAN Potential SSH Scan	1
151.225.152.211	147.237.77.61	United Kingdom	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
114.27.184.221	147.237.0.16	Taiwan	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
151.225.152.211	147.237.76.202	United Kingdom	e.halag.idf.il	ET SCAN Potential SSH Scan	1
105.154.47.147	147.237.77.216	Morocco	dover.idf.il	ETPRO WEB_SERVER PHP Open Flash Charts File Upload Attempt	1

02-23-2016-01:07:05 to 02-23-2016-02:07:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
105.154.47.147	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
105.154.47.147	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	8
120.52.72.42	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
105.154.47.147	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
105.154.47.147	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
105.154.47.147	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.179.20.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.124.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.49.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.134.177	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.57.242	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	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
37.26.148.147	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		alert	2
105.154.47.147	Morocco	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	2
37.26.148.147	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	2
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
40.77.167.88	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.236.26.102	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
192.185.4.39	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
37.26.148.147	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.195	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
146.185.239.102	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.54.153.144	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.236.26.102	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.26.148.187	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.201	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.8.204.67	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.125.71.82	China	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
96.243.254.85	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
46.236.26.102	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
195.228.75.121	Hungary	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.142.143.39	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.202	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.120.80.92	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.3.135.58	Sweden	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.125.71.82	China	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
195.228.75.149	Hungary	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.206	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.111.154.18	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.120.80.92	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.3.144.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.148.147	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.194	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
201.205.49.48	Costa Rica	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	1

02-23-2016-01:07:05 to 02-23-2016-02:07:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-23-2016-01:07:05 to 02-23-2016-02:07:05