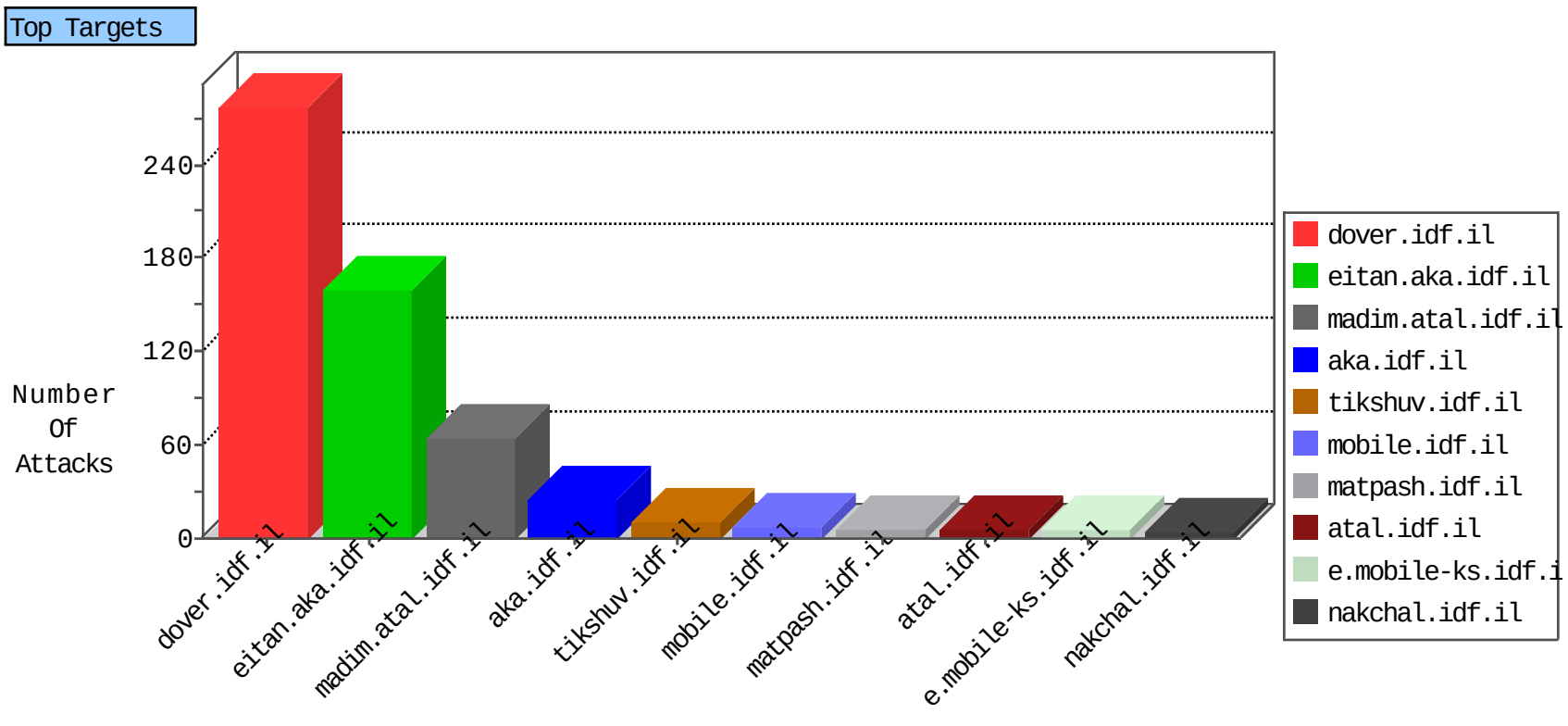
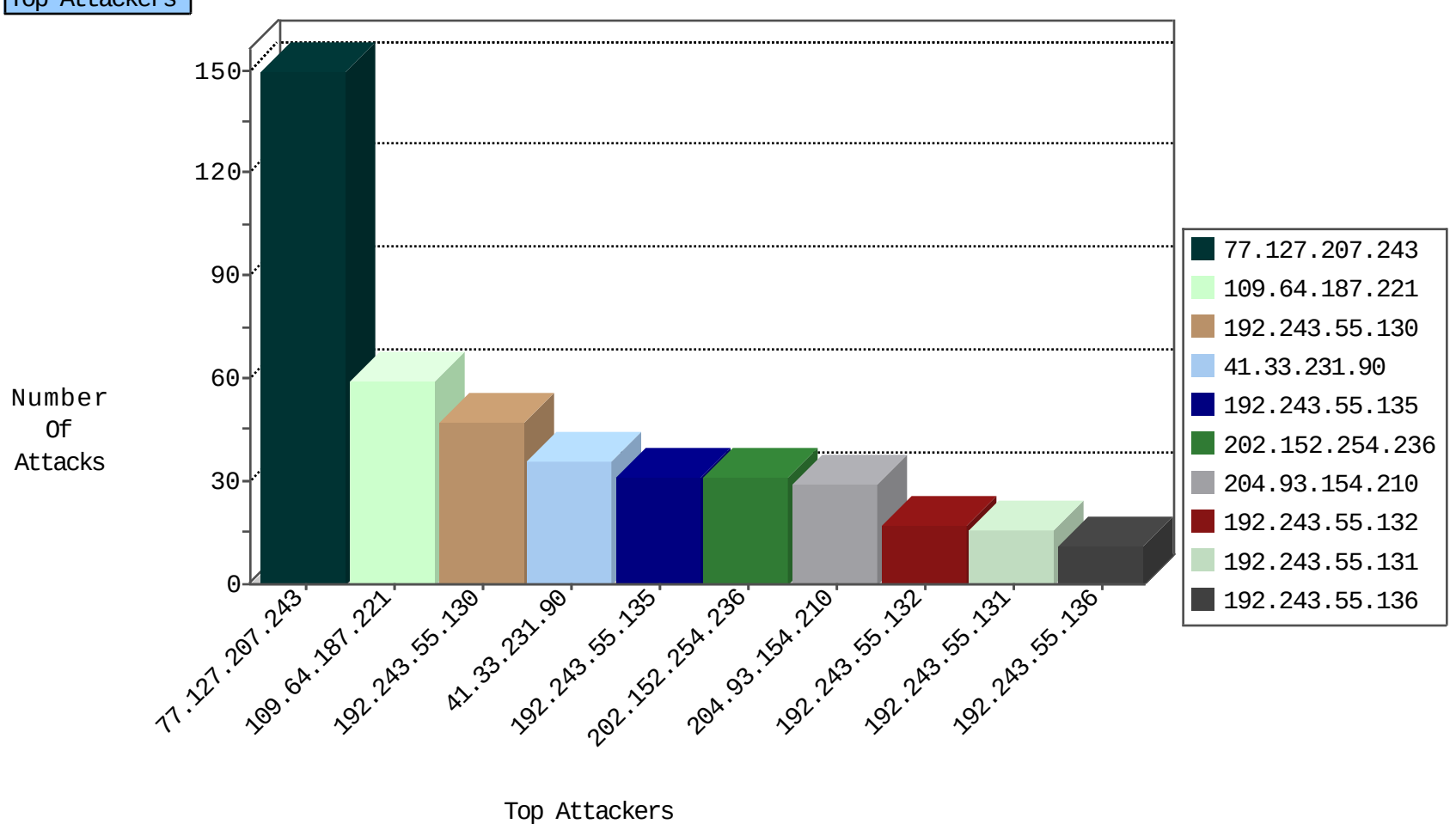
02-21-2016-06:04:00 to 02-21-2016-07:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-21-2016-06:04:00 to 02-21-2016-07:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.154.210	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	198
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
8.37.70.248	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
185.130.5.201		147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.70	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.201		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.70	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1

02-21-2016-06:04:00 to 02-21-2016-07:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.205.0.49	Turkey	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
79.179.124.58	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
157.55.39.97	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
71.231.85.140	United States	147.237.77.216	dover.idf.il	13444: HTTP: WhatWeb User-Agent Header	Block	2
157.55.39.216	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1

02-21-2016-06:04:00 to 02-21-2016-07:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.205.0.49	147.237.72.166	Turkey	aka.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
202.152.254.236	147.237.76.38	Indonesia	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
202.152.254.236	147.237.8.28	Indonesia	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
202.152.254.236	147.237.77.227	Indonesia	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
202.152.254.236	147.237.76.42	Indonesia	refuah.idf.il	ET SCAN Potential SSH Scan	2
202.152.254.236	147.237.8.45	Indonesia	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
202.152.254.236	147.237.77.176	Indonesia	matpash.idf.il	ET SCAN Potential SSH Scan	2
104.209.141.122	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
202.152.254.236	147.237.76.148	Indonesia	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.118	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
74.201.85.87	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
188.213.219.175	147.237.77.205	Romania	prisha.idf.il	ET SCAN Potential SSH Scan	1
202.152.254.236	147.237.8.46	Indonesia	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
41.225.239.16	147.237.76.31	Tunisia	nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
188.213.219.175	147.237.0.33	Romania	idf.il	ET SCAN Potential SSH Scan	1
202.152.254.236	147.237.77.235	Indonesia	sviva.idf.il	ET SCAN Potential SSH Scan	1
41.225.239.16	147.237.76.31	Tunisia	nakchal.idf.il	ET SCAN NMAP -f -sS	1
117.34.116.99	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
202.152.254.236	147.237.0.200	Indonesia	m4u.idf.il	ET SCAN Potential SSH Scan	1
202.152.254.236	147.237.77.170	Indonesia	maarachot.idf.il	ET SCAN Potential SSH Scan	1
117.34.116.99	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
202.152.254.236	147.237.0.33	Indonesia	idf.il	ET SCAN Potential SSH Scan	1
202.152.254.236	147.237.77.19	Indonesia	law-forum.idf.il	ET SCAN Potential SSH Scan	1
117.34.116.99	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
202.152.254.236	147.237.0.16	Indonesia	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
113.59.33.61	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
202.152.254.236	147.237.76.197	Indonesia	e.himush.idf.il	ET SCAN Potential SSH Scan	1
200.82.142.75	147.237.0.35	Venezuela	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.209.141.122	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
202.152.254.236	147.237.76.176	Indonesia	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.118	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
96.82.5.102	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
189.254.90.133	147.237.8.28	Mexico	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
202.152.254.236	147.237.72.156	Indonesia	aman.idf.il	ET SCAN Potential SSH Scan	1
74.201.85.87	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
188.213.219.175	147.237.76.42	Romania	refuah.idf.il	ET SCAN Potential SSH Scan	1
41.225.239.16	147.237.76.31	Tunisia	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
202.152.254.236	147.237.77.234	Indonesia	halag.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.2	147.237.8.46	Russian Federation	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
202.152.254.236	147.237.8.24	Indonesia	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
117.34.116.99	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
202.152.254.236	147.237.0.34	Indonesia	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
202.152.254.236	147.237.77.61	Indonesia	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
117.34.116.99	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
202.152.254.236	147.237.0.17	Indonesia	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
113.59.33.61	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
202.152.254.236	147.237.76.201	Indonesia	e.atal.idf.il	ET SCAN Potential SSH Scan	1
202.152.254.236	147.237.0.15	Indonesia	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.209.141.122	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

02-21-2016-06:04:00 to 02-21-2016-07:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.127.207.243	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	150
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
40.77.167.62	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.26.148.195	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
5.102.254.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
212.29.224.22	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.233	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	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
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
204.93.154.210	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
212.179.224.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
198.20.69.74	United States	147.237.8.28	e.mobile-ks.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
207.46.13.42	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.75.212.89	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
2.54.57.171	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

02-21-2016-06:04:00 to 02-21-2016-07:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.64.187.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
162.243.175.23	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
66.249.78.223	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1749	Block	1
37.26.149.233	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
185.89.217.230		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
131.253.26.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/kkkkkkk=c546ac23kkkkkkk_c546ac23	Block	1
68.180.228.162	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
52.53.255.236	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
185.89.217.233		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
144.76.38.181	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
180.76.15.144	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jeninkilled/stn	Block	1
88.73.8.46	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/an	Block	1
54.183.213.131	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
194.187.168.247	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
157.55.39.215	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
185.89.217.227		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
64.19.78.243	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
157.55.39.226	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/navmenu/	Block	1
66.249.78.216	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1748	Block	1
8.37.70.226	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-18172-he/dover.aspx&usg=alkjrhhzviotopokj5jyxnefqbjezmo2bw	Block	1
185.89.217.229		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
113.76.90.21	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
65.55.218.59	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

02-21-2016-06:04:00 to 02-21-2016-07:04:00