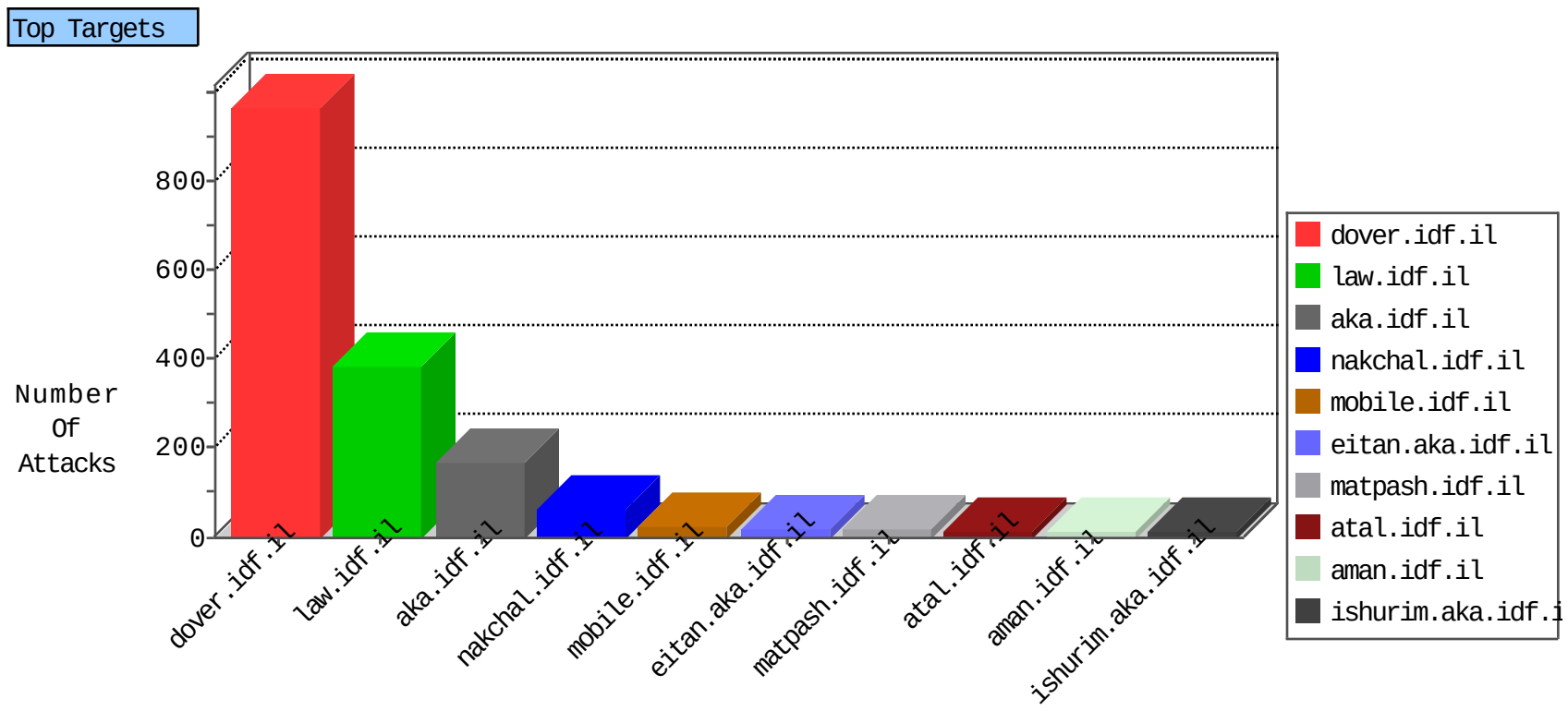
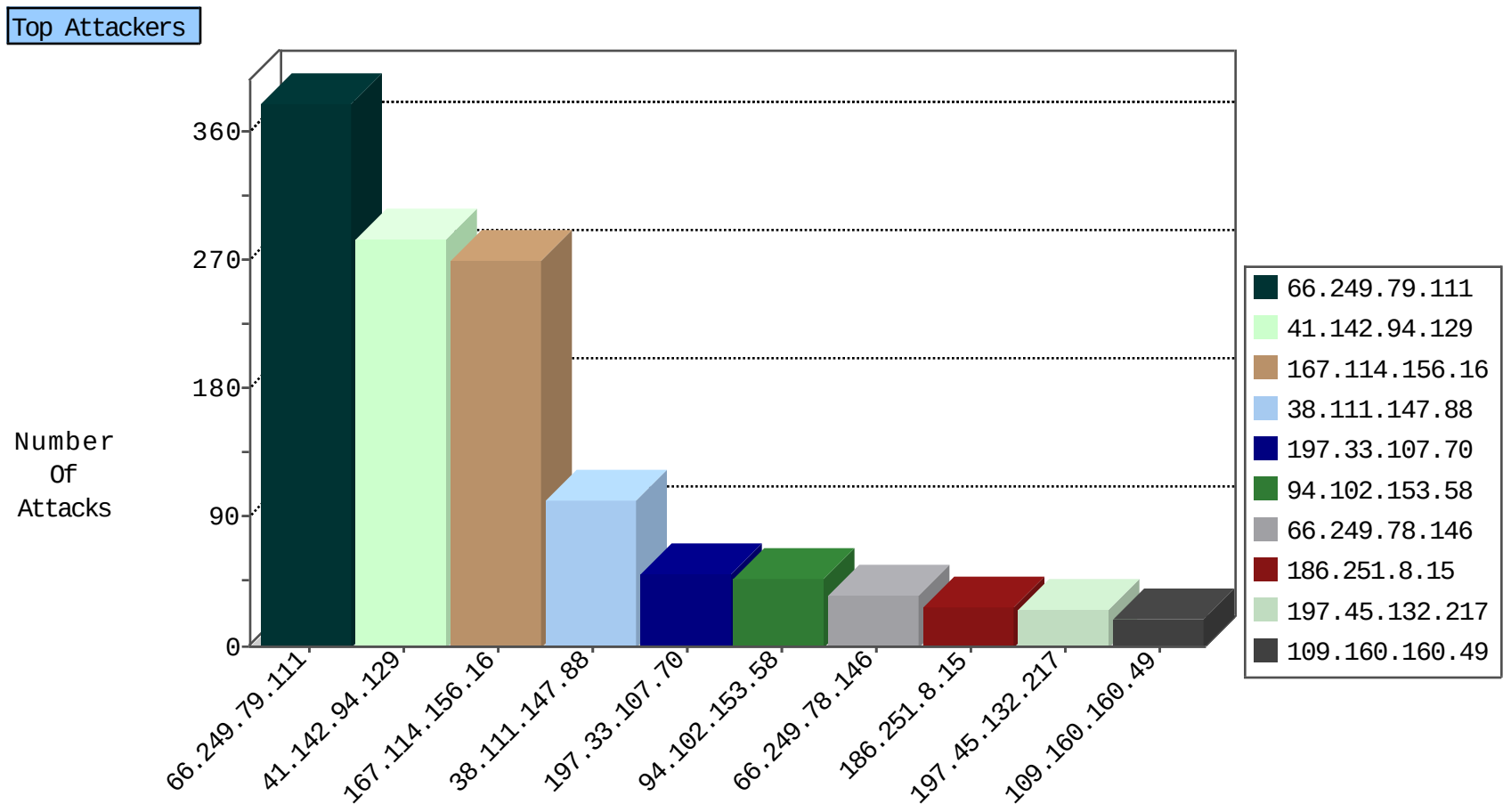
04-25-2016-23:04:02 to 04-26-2016-00:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-25-2016-23:04:02 to 04-26-2016-00:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	11330
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1640
81.218.65.210	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	9
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
107.172.41.5	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.36	China	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
113.17.184.25	China	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
192.249.66.247	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
89.46.102.242	Romania	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
45.63.20.231	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
94.102.52.10	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1

04-25-2016-23:04:02 to 04-26-2016-00:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.102.153.58	United Kingdom	147.237.76.31	nakchal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
94.102.153.58	United Kingdom	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
94.102.153.58	United Kingdom	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4

04-25-2016-23:04:02 to 04-26-2016-00:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.79.111	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	380
94.102.153.58	147.237.76.31	United Kingdom	nakchal.idf.il	SQL Injection - Select From	36
109.160.160.49	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	12
41.142.94.129	147.237.77.216	Morocco	dover.idf.il	SERVER-WEBAPP login.htm access	12
41.142.94.129	147.237.77.216	Morocco	dover.idf.il	SERVER-WEBAPP admin.php access	10
41.142.94.129	147.237.77.216	Morocco	dover.idf.il	SERVER-WEBAPP adminlogin access	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
186.251.8.15	147.237.8.46	Brazil	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
174.37.194.144	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sA (2)	2
186.251.8.15	147.237.76.176	Brazil	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
197.33.107.70	147.237.77.216	Egypt	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.88.81	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
186.251.8.15	147.237.77.243	Brazil	mobile.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.233	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
186.251.8.15	147.237.76.44	Brazil	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
195.154.54.169	147.237.76.202	France	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
186.251.8.15	147.237.76.34	Brazil	yohalan.idf.il	ET SCAN Potential SSH Scan	1
78.183.33.118	147.237.77.216	Turkey	dover.idf.il	SERVER-WEBAPP admin.php access	1
190.29.116.141	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
186.251.8.15	147.237.77.233	Brazil	atal.idf.il	ET SCAN Potential SSH Scan	1
186.251.8.15	147.237.8.27	Brazil	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
186.251.8.15	147.237.77.226	Brazil	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
186.251.8.15	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Potential SSH Scan	1
186.251.8.15	147.237.77.170	Brazil	maarachot.idf.il	ET SCAN Potential SSH Scan	1
186.251.8.15	147.237.0.33	Brazil	idf.il	ET SCAN Potential SSH Scan	1
186.251.8.15	147.237.76.200	Brazil	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
13.92.122.143	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
186.251.8.15	147.237.0.15	Brazil	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
186.251.8.15	147.237.76.197	Brazil	e.himush.idf.il	ET SCAN Potential SSH Scan	1
217.72.245.216	147.237.76.86	United Kingdom	navy.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
109.235.254.181	147.237.77.74	Turkey	law.idf.il	ET SCAN NMAP -sS window 3072	1
186.251.8.15	147.237.76.38	Brazil	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
186.251.8.15	147.237.76.31	Brazil	nakchal.idf.il	ET SCAN Potential SSH Scan	1
186.251.8.15	147.237.8.45	Brazil	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
186.251.8.15	147.237.77.227	Brazil	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
186.251.8.15	147.237.0.200	Brazil	m4u.idf.il	ET SCAN Potential SSH Scan	1
186.251.8.15	147.237.77.205	Brazil	prisha.idf.il	ET SCAN Potential SSH Scan	1
186.251.8.15	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
186.251.8.15	147.237.77.61	Brazil	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
13.92.122.143	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
186.251.8.15	147.237.0.16	Brazil	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
186.251.8.15	147.237.76.199	Brazil	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
13.92.122.143	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
220.88.41.2	147.237.0.17	Korea, Republic of	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
186.251.8.15	147.237.76.196	Brazil	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
109.235.254.181	147.237.77.74	Turkey	law.idf.il	ET SCAN NMAP -sS window 4096	1
201.166.223.4	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

04-25-2016-23:04:02 to 04-26-2016-00:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	103
197.33.107.70	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	35
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
37.26.148.181	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.6.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.18.142.45	Italy	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
100.36.28.116	United States	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
45.59.183.143	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.11	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
157.55.39.74	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
88.191.204.49	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
80.246.130.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.143	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
86.104.164.250	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
87.70.79.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.67.189.48	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.191	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.177.98.163	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
157.55.39.130	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.46.13.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.88.152.231	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.96.128.60	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
46.19.85.46	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.88.152.231	Saudi Arabia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
174.37.194.144	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
37.142.68.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.10.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
213.8.204.67	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
188.120.154.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.149.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
64.9.57.180	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.60.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
132.72.212.210	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.64.145.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.6.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
140.198.52.206	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.65.234.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.136.153	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

04-25-2016-23:04:02 to 04-26-2016-00:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.142.94.129	Morocco	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.142.94.129	Block	96
41.142.94.129	Morocco	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	91
41.142.94.129	Morocco	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	70
84.110.35.134	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	8
78.183.33.118	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 78.183.33.118	Block	6
2.53.154.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
2.53.166.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
78.183.33.118	Turkey	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	5
109.160.160.49	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.160.160.49	Block	5
75.62.18.194	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/homepage/mobile	Block	4
78.183.33.118	Turkey	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 78.183.33.118	Block	4
8.37.232.39	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
71.172.34.80	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/general/mobile	Block	2
109.160.160.49	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/general/	Block	2
89.142.181.78	Slovenia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
2.53.27.5	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/general/mobile	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/size100x0/3392.jpg	Block	1
109.253.136.153	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
78.183.33.118	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
71.172.34.80	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/homepage/mobile	Block	1
46.19.85.143	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
185.3.147.184	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/rules.abe	Block	1
90.183.7.250	Czech Republic	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
78.183.33.118	Turkey	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
217.72.245.216	United Kingdom	147.237.76.86	navy.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.66.152	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
117.78.13.29	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
79.183.160.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
65.55.210.56	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.120.125.10	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
90.183.7.250	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
66.249.66.156	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1501-he/atal.aspx	Block	1
140.198.52.206	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	1
82.166.228.10	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
71.206.247.142	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
190.210.38.17	Argentina	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
5.9.89.170	Germany	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1105-en/contactus.aspx	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/forgotpassword.aspx	Block	1
157.55.2.185	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
75.62.18.194	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/general/mobile	Block	1
207.46.13.13	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/1055-he.patzar.aspx	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
5.28.151.247	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/news/mobile	Block	1
69.159.55.34	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
46.19.85.11	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1

04-25-2016-23:04:02 to 04-26-2016-00:04:02