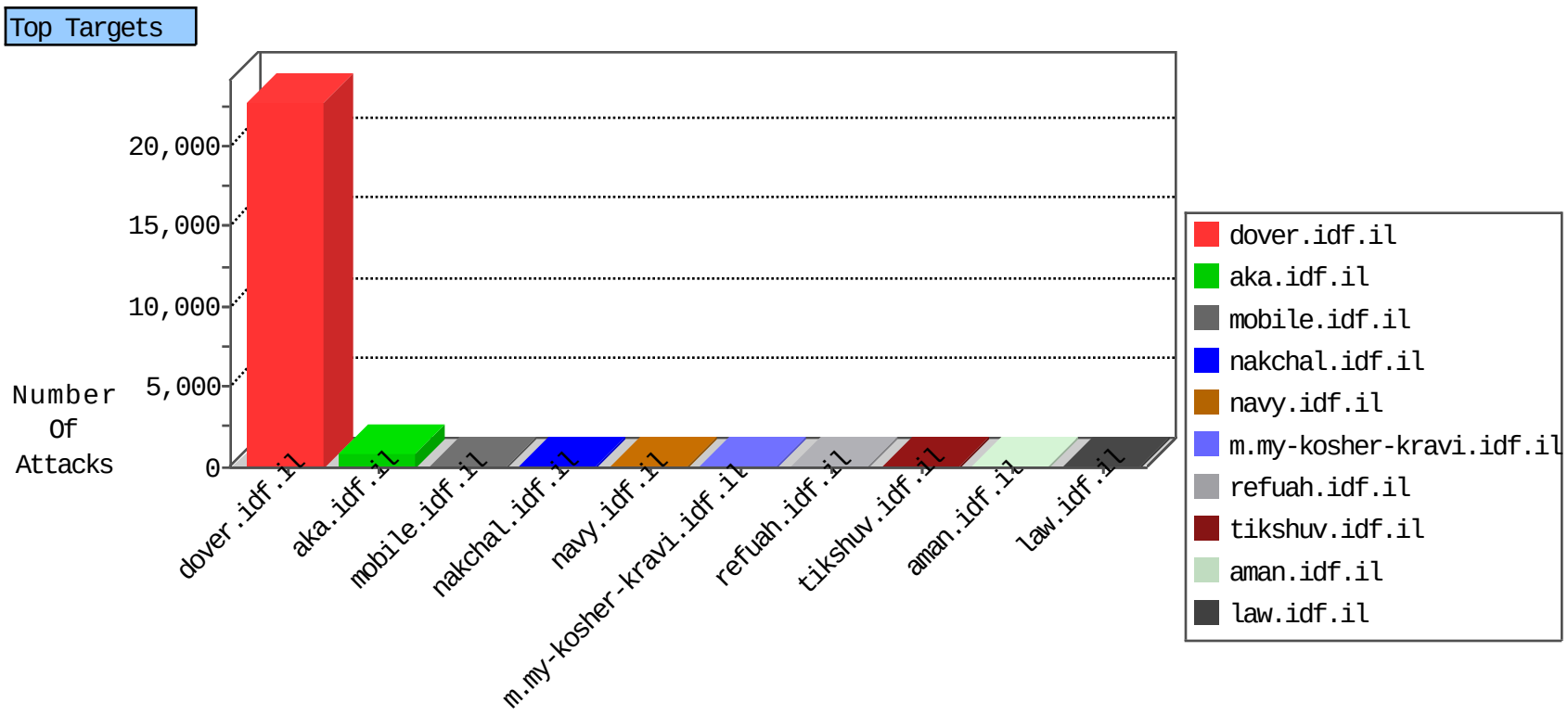
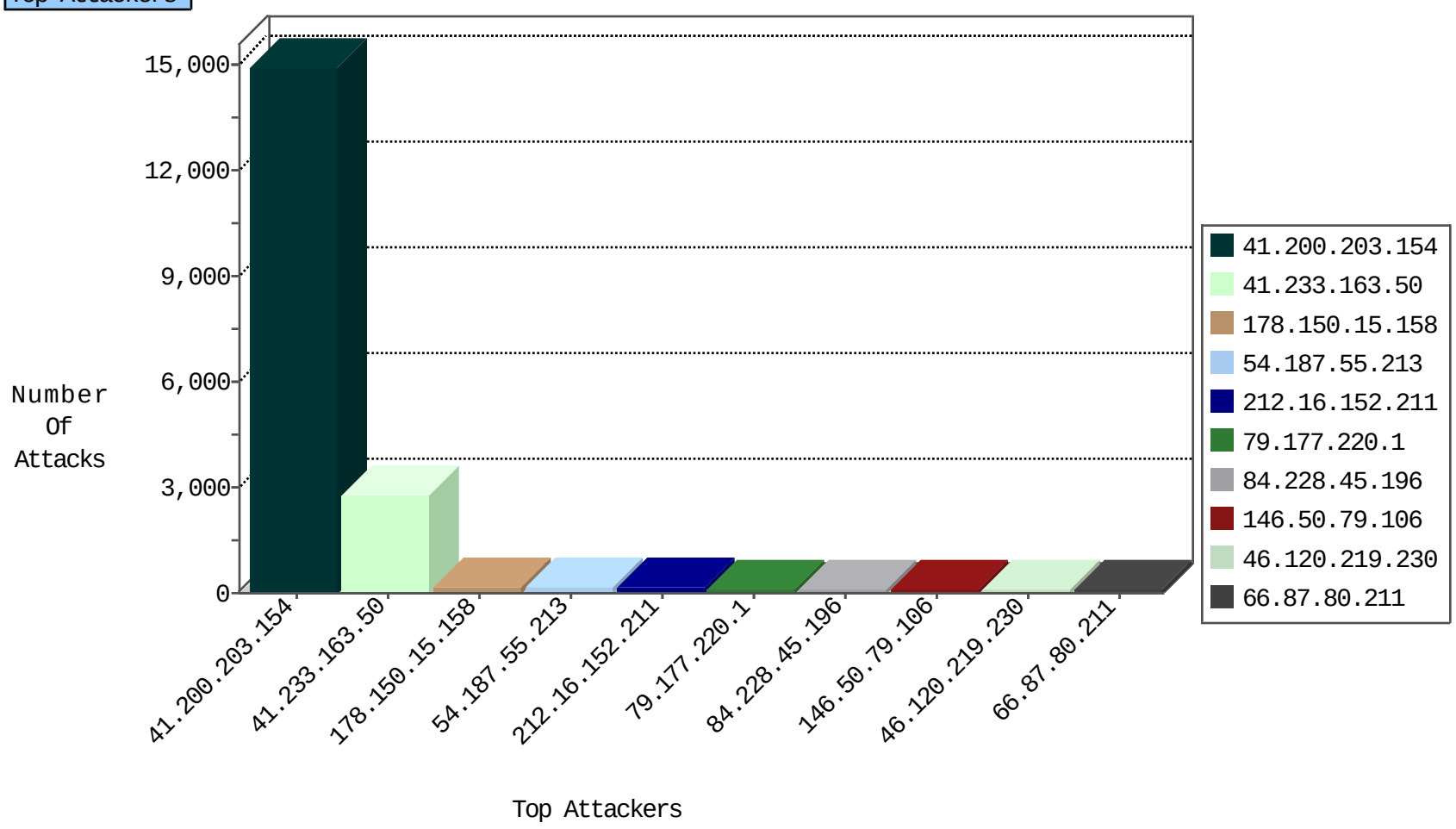
10-31-2015-21:04:05 to 10-31-2015-22:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-31-2015-21:04:05 to 10-31-2015-22:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.27.150	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2648
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	673
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	224
220.181.108.107	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	164
41.233.163.50	Egypt	147.237.77.216	dover.idf.il	Web-etc/passwd-Dir-Traversal	dest-reset	87
79.181.98.122	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	73
5.22.130.79	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	46
84.110.33.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
5.22.129.200	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
80.246.136.49	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
79.181.183.188	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
84.109.176.82	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
109.186.59.14	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
84.108.215.64	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
109.66.191.70	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	17
46.19.85.225	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
212.179.225.218	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
79.181.96.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
46.19.85.225	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
15.203.233.76	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
77.127.53.247	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
87.69.160.97	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
89.138.227.255	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
46.121.150.97	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
79.176.8.80	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
94.230.86.135	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
79.182.222.104	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
37.26.147.223	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.210.142.176	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
84.228.215.141	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
37.26.147.130	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
5.22.129.136	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
5.29.88.158	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
31.168.13.78	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.54.151.226	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.86.114	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
66.102.8.242	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
84.109.165.231	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
5.22.129.247	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.86.236	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.177.202.96	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
31.44.138.115	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.182.189.167	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
87.69.106.254	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
66.102.8.237	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
149.78.6.59	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
87.69.149.180	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
37.142.64.2	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.85.221	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
46.120.219.230	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4

10-31-2015-21:04:05 to 10-31-2015-22:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.228.45.196	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
41.233.163.50	Egypt	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

10-31-2015-21:04:05 to 10-31-2015-22:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	SQL Injection - Select From	197
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	173
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	127
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	SQL 1 = 1 - possible sql injection attempt	123
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	GPL WEB_SERVER /etc/passwd	106
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	94
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	ET WEB_SERVER /bin/sh In URI Possible Shell Command Execution Attempt	94
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	94
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	SQL url ending in comment characters - possible sql injection attempt	94
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	ET WEB_SERVER cmd.exe In URI - Possible Command Execution Attempt	94
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt	94
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	SERVER-WEBAPP /etc/passwd file access attempt	94
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	SERVER-IIS cmd.exe access	94
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	SQL union select - possible sql injection attempt - GET parameter	84
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	84
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access	79
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	ET WEB_SERVER Onmouseover= in URI - Likely Cross Site Scripting Attempt	62
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	SERVER-WEBAPP TRACE attempt	52
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	GPL WEB_SERVER .htaccess access	32
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	SERVER-WEBAPP .htaccess access	32
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	SQL union select - possible sql injection attempt - POST parameter	4
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	SQL Injection - Union Select (POST)	4
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	SQL Injection - Select From (POST)	4
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	SQL Injection - Union (POST)	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.i	Tehila - Perl LWP with fake user agent	4
195.34.150.18	147.237.77.216	Austria	dover.idf.i	Tehila - Perl LWP with fake user agent	3
41.233.163.50	147.237.77.216	Egypt	dover.idf.i	SQL Injection - Paranoid	1

10-31-2015-21:04:05 to 10-31-2015-22:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.200.203.154	Algeria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14922
41.233.163.50	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	761
54.187.55.213	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	148
212.16.152.211	Hungary	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	143
79.177.220.1	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	115
146.50.79.106	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	105
46.120.219.230	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	82
66.87.80.211	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	77
46.19.85.112	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	72
79.178.18.119	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	60
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	58
46.153.176.163	Saudi Arabia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	55
79.179.210.203	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	53
82.166.22.77	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	52
94.230.86.135	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
176.13.5.105	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	50
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	47
176.13.10.25	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	47
46.19.86.133	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	45
64.233.172.171	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
79.181.183.188	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
190.21.108.244	Chile	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
141.0.14.210	Europe	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
46.19.85.225	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
79.177.8.151	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
176.13.3.204	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
79.181.168.62	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
64.233.172.163	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
149.78.241.169	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	31
66.102.8.243	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
85.130.231.248	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
5.29.203.75	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
66.249.81.218	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
41.200.203.154	Algeria	147.237.77.216	dover.idf.i	drop		drop	27
100.100.5.84		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	27
109.65.33.176	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
5.22.130.79	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
84.109.165.231	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
46.19.86.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
85.130.140.60	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
85.104.36.151	Turkey	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
46.19.86.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
128.242.249.13	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24

10-31-2015-21:04:05 to 10-31-2015-22:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
178.150.15.158	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	90
178.150.15.158	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 178.150.15.158	Block	75
195.182.94.10	Lithuania	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 195.182.94.10	Block	60
109.66.149.62	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.66.149.62	Block	60
84.228.45.196	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	45
5.22.130.105	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	44
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	30
89.138.70.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	30
84.228.45.196	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 84.228.45.196	Block	30
79.179.178.135	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	30
80.230.17.78	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	29
2.54.130.212	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site	Block	15
85.250.230.212	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	15
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/2880.pdf	Block	15
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
134.0.11.76	Spain	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/test/wp-admin/	Block	15
31.154.91.48	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 31.154.91.48 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	15
66.249.75.54	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	15
46.19.86.66	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
5.22.129.166	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	15
79.176.153.111	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
151.80.31.112	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
37.8.17.129	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	15
66.249.75.70	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/8/228.pdf	Block	15
46.117.20.169	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	15
5.22.129.220	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	15
93.172.142.250	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	15
195.182.94.10	Lithuania	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/	Block	15
157.55.39.171	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	15
37.26.149.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
46.117.20.169	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/talpiotquestionnaire.aspx	None	15
178.150.15.158	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	15
79.181.140.206	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	15
199.16.128.53	Canada	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp-admin/	Block	15
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	15
176.13.10.24	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
41.233.163.50	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/nosuchpage123	Block	15
84.228.45.196	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	15
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	15
46.121.139.122	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	15
185.32.179.76	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	15
109.66.149.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	15
5.144.60.113	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar	Block	15
79.182.189.167	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	15
207.46.13.57	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/brothers/kishur/default.asp	None	15
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	15
176.13.19.243	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/1923.pdf	Block	15

10-31-2015-21:04:05 to 10-31-2015-22:04:05