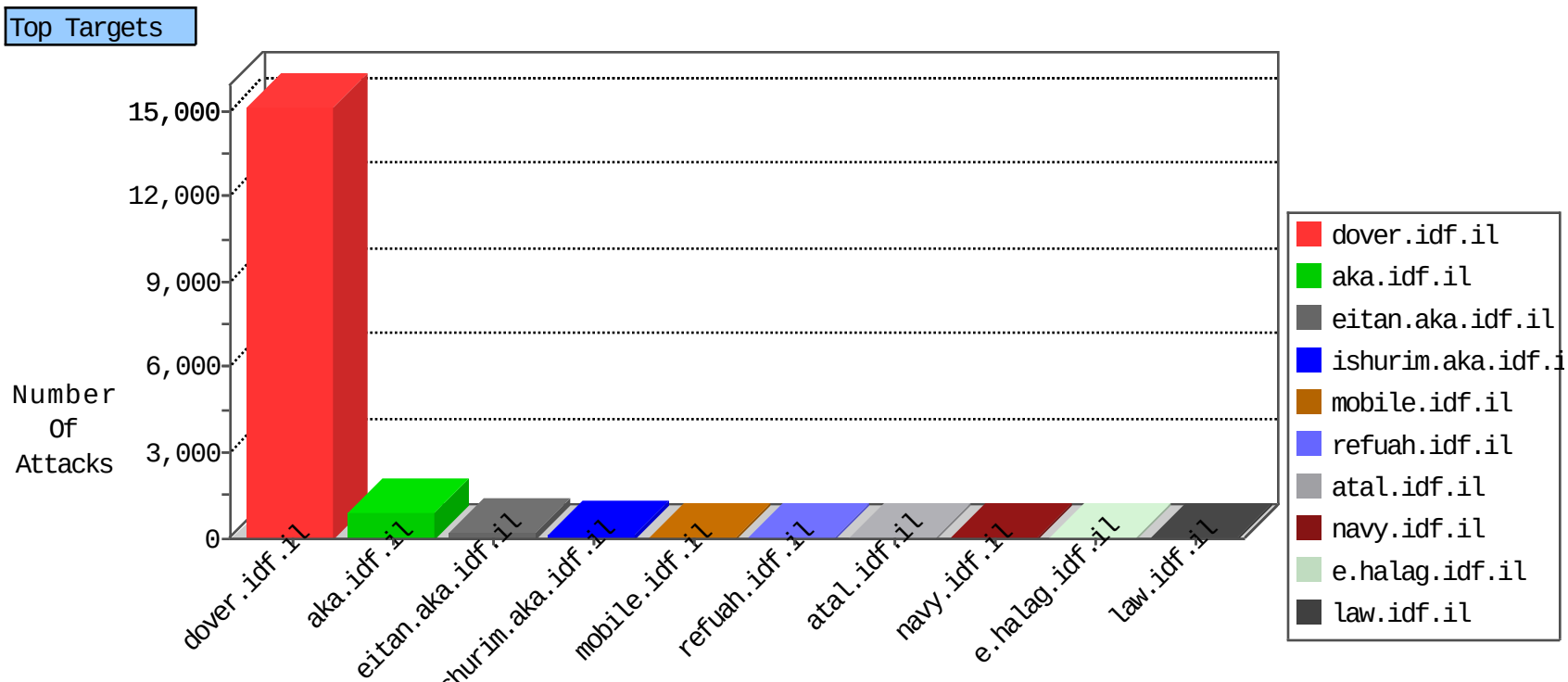
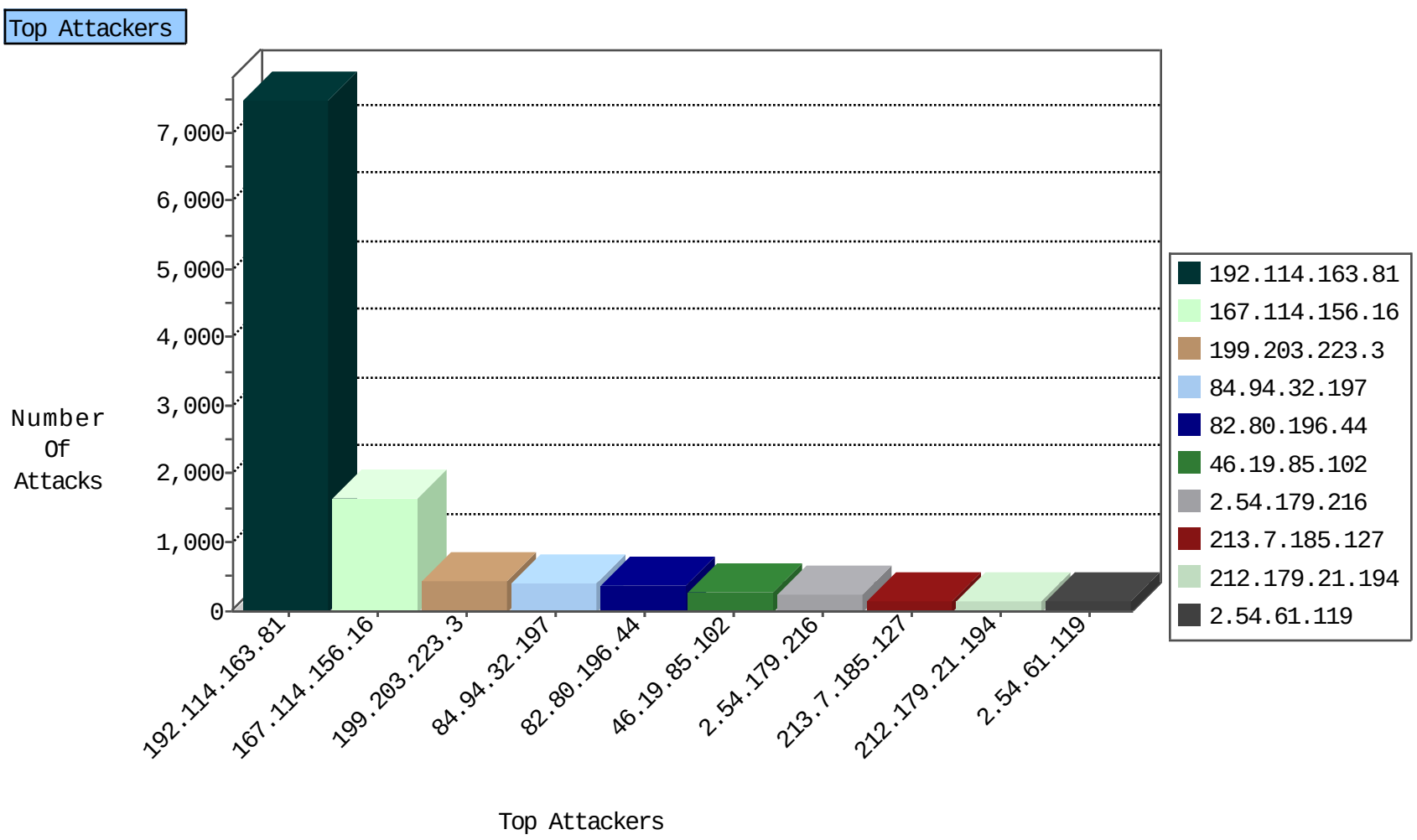
11-02-2015-12:04:02 to 11-02-2015-13:04:02

IDF Under Attack
Daily Report





11-02-2015-12:04:02 to 11-02-2015-13:04:02

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	DOS-Tool-SwitchbladG	dest-reset	2752
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	487
192.114.163.81	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	98
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	66
95.86.69.152	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	52
194.90.132.29	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	33
46.116.252.23	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
131.111.184.92	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
66.27.195.251	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
2.54.5.175	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
132.73.195.185	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
46.19.85.102	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
79.180.51.2	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
2.52.40.1	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
66.27.195.251	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
176.13.14.108	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
73.231.208.33	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
192.116.172.33	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
79.182.56.68	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
93.173.0.99	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.54.57.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
37.142.155.3	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.176.224.26	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.12.145.223	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.21.32	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
95.86.65.190	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.106.46.88	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.67.104.57	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.85.244	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
62.219.187.57	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
80.179.197.157	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
82.80.219.164	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
81.218.116.129	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
49.80.172.1	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	3
81.218.206.82	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
87.68.17.215	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
95.35.148.121	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
79.177.121.201	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
46.19.86.14	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
212.76.124.221	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
80.179.197.157	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
185.32.179.14	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
37.26.147.160	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
212.179.71.70	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
192.116.160.52	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.85.102	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
93.145.255.154	Italy	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
212.143.233.210	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2

11-02-2015-12:04:02 to 11-02-2015-13:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.228.109.215	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
164.138.121.176	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

11-02-2015-12:04:02 to 11-02-2015-13:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.61.218.123	147.237.76.198	Germany	e.yohalan.idf.il	ET SCAN NMAP -sA (2)	2
46.19.85.117	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
212.7.209.9	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.52.4.48	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.114.163.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
173.69.138.60	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
95.86.101.195	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.160.196	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.12.202.110	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
79.176.131.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
54.72.73.168	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
213.61.218.123	147.237.76.39	Germany	mobile.meitav.idf.il	ET SCAN NMAP -sA (2)	1
37.26.146.247	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.76.124.221	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.190.25	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
185.24.207.16	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.67.104.175	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.130.228.237	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.34.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.61.218.123	147.237.76.200	Germany	eitan.aka.idf.il	ET SCAN NMAP -sA (2)	1
66.249.67.224	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
213.61.218.123	147.237.76.44	Germany	e.refuah.idf.il	ET SCAN NMAP -sA (2)	1

11-02-2015-12:04:02 to 11-02-2015-13:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.114.163.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7482
199.203.223.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	456
84.94.32.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	387
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	383
2.54.179.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	256
46.19.85.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	248
213.7.185.127	Cyprus	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	142
2.54.61.119	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	135
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	128
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	121
109.64.212.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
46.19.86.64	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
212.68.153.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
41.182.0.123	Namibia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
46.19.86.72	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
105.196.8.206	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
89.139.6.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
66.249.83.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
46.121.211.156	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
41.218.185.199	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
2.52.141.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
95.188.197.127	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
131.111.184.92	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
79.180.51.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
95.86.124.12	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
46.19.86.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.116.236.48	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
46.19.86.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.86.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
93.173.0.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
66.249.78.159	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
2.52.43.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
121.210.88.46	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
37.26.146.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
46.117.128.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
188.225.185.133	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
62.0.34.177	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	25
82.80.219.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
66.249.78.166	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24

11-02-2015-12:04:02 to 11-02-2015-13:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.83.210	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	8
80.246.136.62	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	4
80.246.137.191	Israel	147.237.76.39	mobile.meitav.idf.il	Cookie Tampering on cookie .ASPNETAUTH: Expected 0102E8CAF92370E3D208FEE8423BEF72E3D208000932003000380036003400350039003700380000012F00FF, Observed 0102086153B476D8D208FE08D9947F79D8D208000932003000380036003400350039003700380000012F00FF	None	3
176.13.4.245	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
82.166.140.117	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
176.13.14.216	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.142.143.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.83.214	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
31.168.6.66	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/2/111872.pdf	Block	2
2.54.171.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.83.218	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
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	2
62.219.131.163	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/kesher	Block	1
37.142.64.119	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/lomdim/forum/	Block	1
212.179.21.197	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
80.74.107.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/ajax/updatestatus.php	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
23.91.70.109	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
94.199.238.15	United Kingdom	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
2.52.21.50	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.19.86.244	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
37.26.148.137	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.118.128.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
74.6.53.168	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
2.54.136.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.185	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/giyus/qanda/default.asp	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.13	Block	1
84.228.50.175	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.101.50.168	Netherlands	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	1
213.8.67.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
23.96.208.27	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
176.13.20.16	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.52.23.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.64.148.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/talpiotquestionnarie.aspx	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
46.120.115.210	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.120.115.210	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.26.148.207	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/17468.jpg	Block	1
79.179.209.106	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.155.236	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
176.12.142.226	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1150-he/chinuch.aspx	Block	1
84.229.197.247	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
80.179.96.90	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/tizmoret/faq/default.asp	None	1
46.19.85.2	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
185.120.126.33		147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
2.54.34.145	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1

11-02-2015-12:04:02 to 11-02-2015-13:04:02