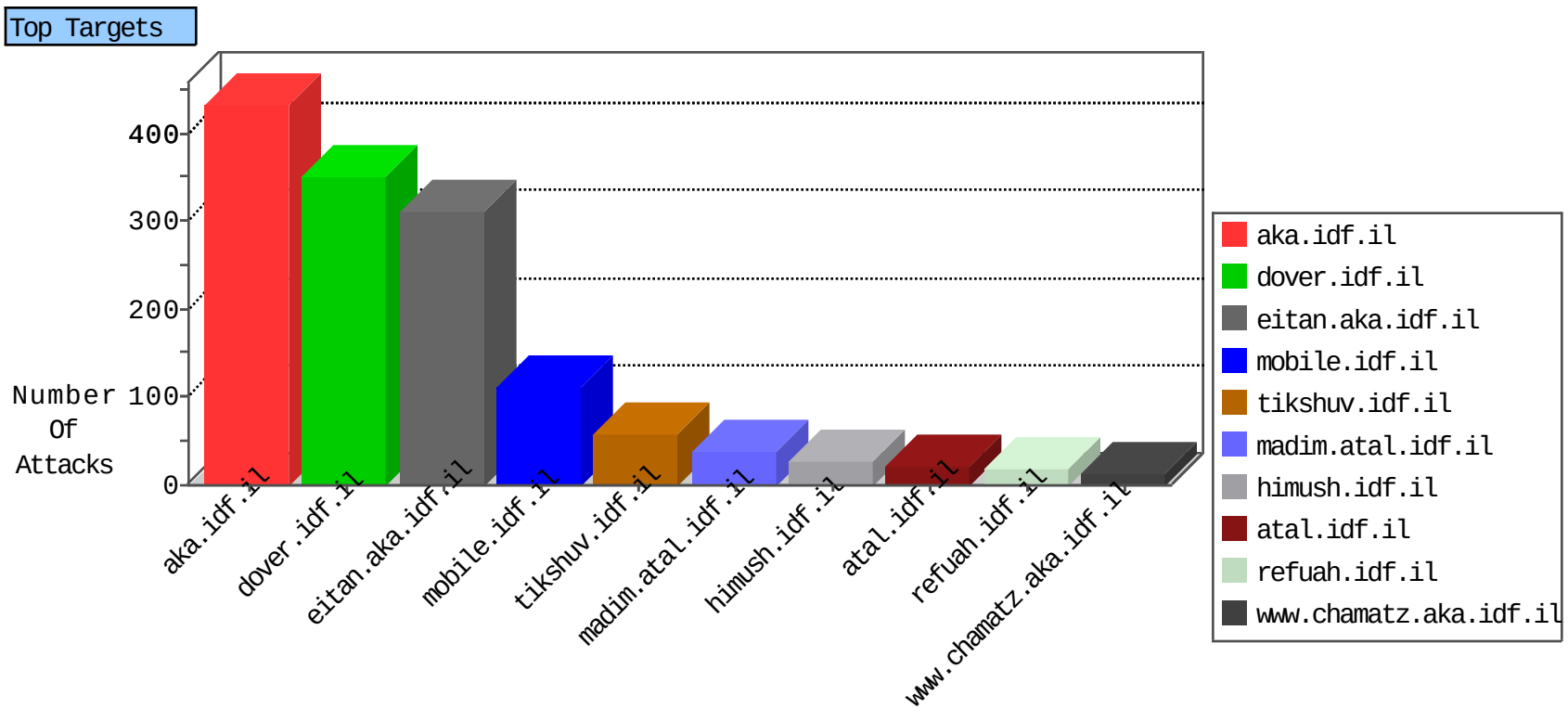
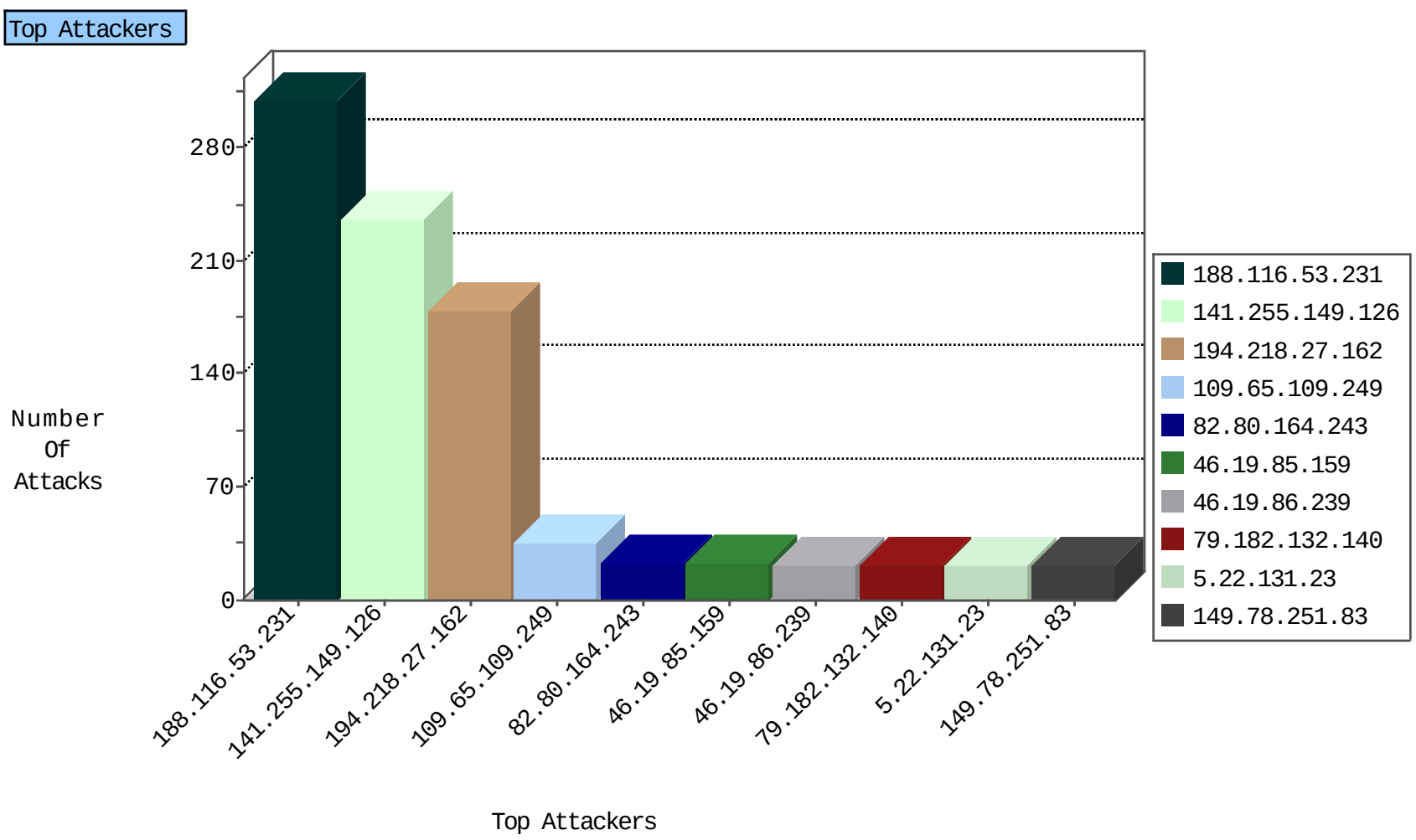
03-01-2016-22:04:02 to 03-01-2016-23:04:02

IDF Under Attack
Daily Report





03-01-2016-22:04:02 to 03-01-2016-23:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.255.149.126	Netherlands	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1000
66.249.66.105	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	139
109.65.181.46	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
82.145.210.189	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
42.112.10.87	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
42.112.10.83	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
188.138.102.50	Germany	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
42.112.10.75	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
120.108.22.50	Taiwan	147.237.72.14	dover.idf.il(old)	Block_Udp_All_Nets	drop	1
42.112.10.84	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
208.67.1.70	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
42.112.10.80	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
42.112.10.85	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
109.65.181.46	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
42.112.10.81	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
188.138.102.50	Germany	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

03-01-2016-22:04:02 to 03-01-2016-23:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.109.249	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
188.116.53.231	Poland	147.237.76.200	eitan.aka.idf..	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	12
188.116.53.231	Poland	147.237.76.200	eitan.aka.idf..	22095: HTTP: Joomla Image Manager folderRename Security Bypass Vulnerability	Block	12
217.227.76.195	Germany	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
106.38.241.107	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
79.178.217.6	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
176.228.166.188	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
62.212.73.211	Netherlands	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.203.166	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
136.243.152.18	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
217.132.120.251	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
198.23.176.146	United States	147.237.76.86	navy.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-01-2016-22:04:02 to 03-01-2016-23:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
188.116.53.231	147.237.76.200	Poland	eitan.aka.idf.il	Tehila - Perl LWP with fake user agent	76
188.116.53.231	147.237.76.200	Poland	eitan.aka.idf.il	SERVER-WEBAPP Mambo upload.php access	40
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	9
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
113.76.90.199	147.237.77.179	China	e.mazi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
5.29.145.111	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.193.176	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
98.119.105.221	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
95.173.184.12	147.237.76.38	Turkey	e.e.meitav.idf.i	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
93.87.16.148	147.237.76.44		e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
195.216.176.244	147.237.77.216	Latvia	dover.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.169.37	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
63.221.141.195	147.237.0.34	Hong Kong	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
164.138.122.209	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
45.56.98.150	147.237.8.24		e.lifestyle.idf	ET SCAN Potential SSH Scan	1
146.185.250.2	147.237.72.217	Russian Federation	e.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.68.137	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
113.76.90.199	147.237.8.45	China	e.eitan.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
98.119.105.221	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 2048	1
98.119.105.221	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -f -sS	1
218.246.0.97	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.91.29	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
93.87.16.148	147.237.0.33		idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.177.115.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.120.240.238	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.199.177	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

03-01-2016-22:04:02 to 03-01-2016-23:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	119
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	60
82.80.164.243	Israel	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	23
5.22.131.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
109.65.109.249	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
79.182.132.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
149.78.251.83	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.117.179.164	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
46.19.86.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
213.57.139.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
81.4.163.106	Cyprus	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.198	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.183.178.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.232	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
105.107.114.78	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.18	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
87.79.69.115	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.223	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.17.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.255.149.126	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.182.26.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.12	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.157.176	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.51.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.202.69	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.223	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
217.132.55.7	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	4
87.70.62.77	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	4
5.102.195.220	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.62.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.86.1	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.105.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.210.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.132.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.179.195.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.142.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.182.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.223	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.54.61.90	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-01-2016-22:04:02 to 03-01-2016-23:04:02

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.177.179.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.121.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.1.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.223	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.64.22.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.194.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.116.53.231	Poland	147.237.76.200	eitan.aka.idf.il	Distributed PHP Attempt	Block	76
188.116.53.231	Poland	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 188.116.53.231	Block	75
46.19.85.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	23
188.116.53.231	Poland	147.237.76.200	eitan.aka.idf.il	Multiple signatures from 188.116.53.231	Block	18
62.219.193.62	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 62.219.193.62	Block	9
46.19.86.239	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
176.13.1.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.109.14.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
149.78.251.83	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.183.235	Block	2
87.79.69.115	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	2
27.32.6.167	Australia	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.54.28.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.130.248	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
94.199.151.22	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 94.199.151.22	Block	2
46.19.85.198	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
95.86.69.38	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-14027-he/dover.aspx&sa=u&ved=0ahukewjrivpuq6dlahuk2b4khcllcloqfggnmae&usg=afqjcnhd5dfli3rr6oo6_4yhyhnayzyieg	Block	1
54.213.177.200	United States	147.237.72.166	aka.idf.il	NULL Character in Method	Block	1
46.117.179.164	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
79.177.115.227	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/4/size338x0/1584.jpg	Block	1
2.54.167.223	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
66.102.7.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
120.37.204.206	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 120.37.204.206	Block	1
50.93.198.232	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/7/307.pdf/xmlrpc.php	Block	1
84.111.30.103	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
40.77.167.9	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/unselecatble.aspx	Block	1
2.54.26.5	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
157.55.39.104	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
68.94.1.7	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
54.213.177.200	United States	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in Method	Block	1
95.132.175.9	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/0/size220x0/9020.jpg	Block	1
46.121.156.188	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
79.183.178.206	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.102.7.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
120.37.204.206	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
89.138.59.101	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	1
50.93.198.232	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 50.93.198.232	Block	1
84.111.30.103	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.111.30.103	Block	1
77.126.171.84	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
54.213.177.200	United States	147.237.77.176	matpash.idf.il	NULL Character in Method	Block	1
109.67.15.93	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.121.156.188	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.121.156.188	Block	1
85.167.117.181	Norway	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
37.203.214.2	Sweden	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
188.116.53.231	Poland	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/index.php	Block	1
123.125.71.81	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	1
66.102.7.240	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
50.93.198.232	United States	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1