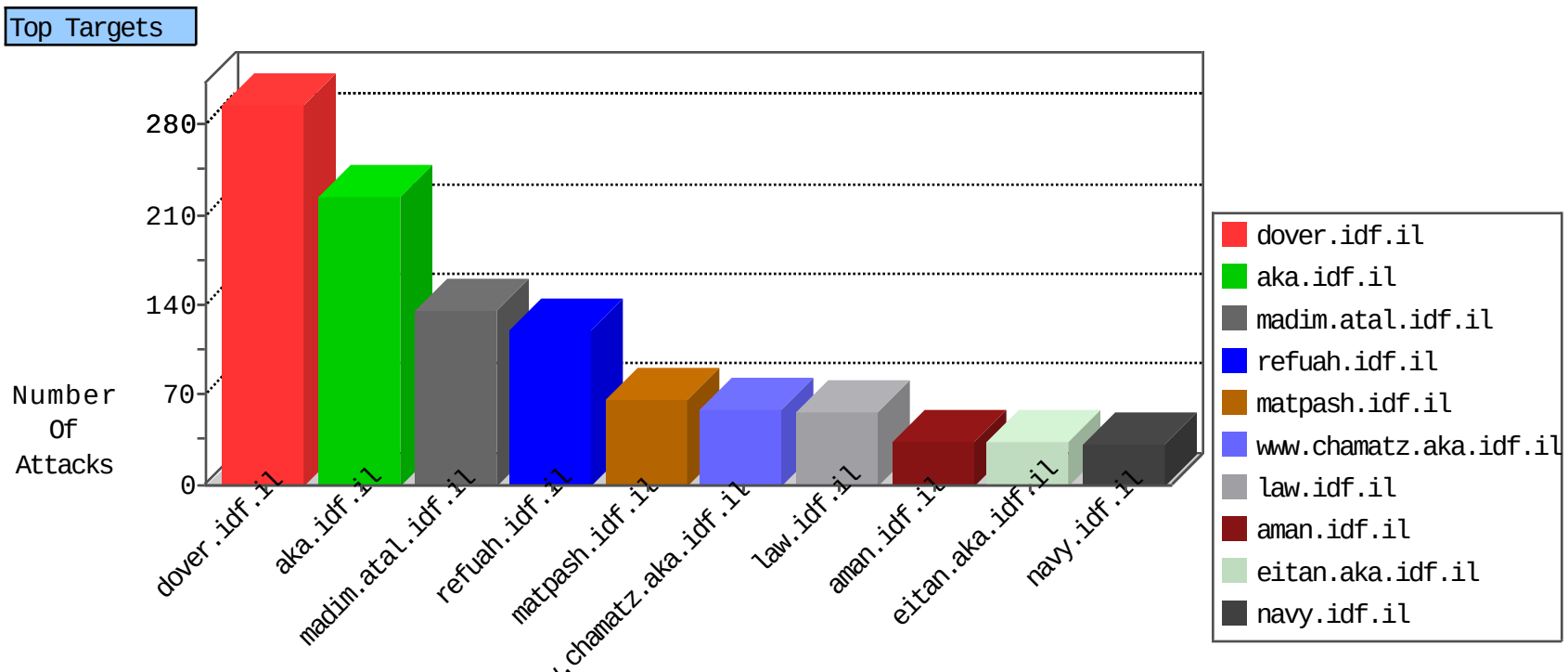
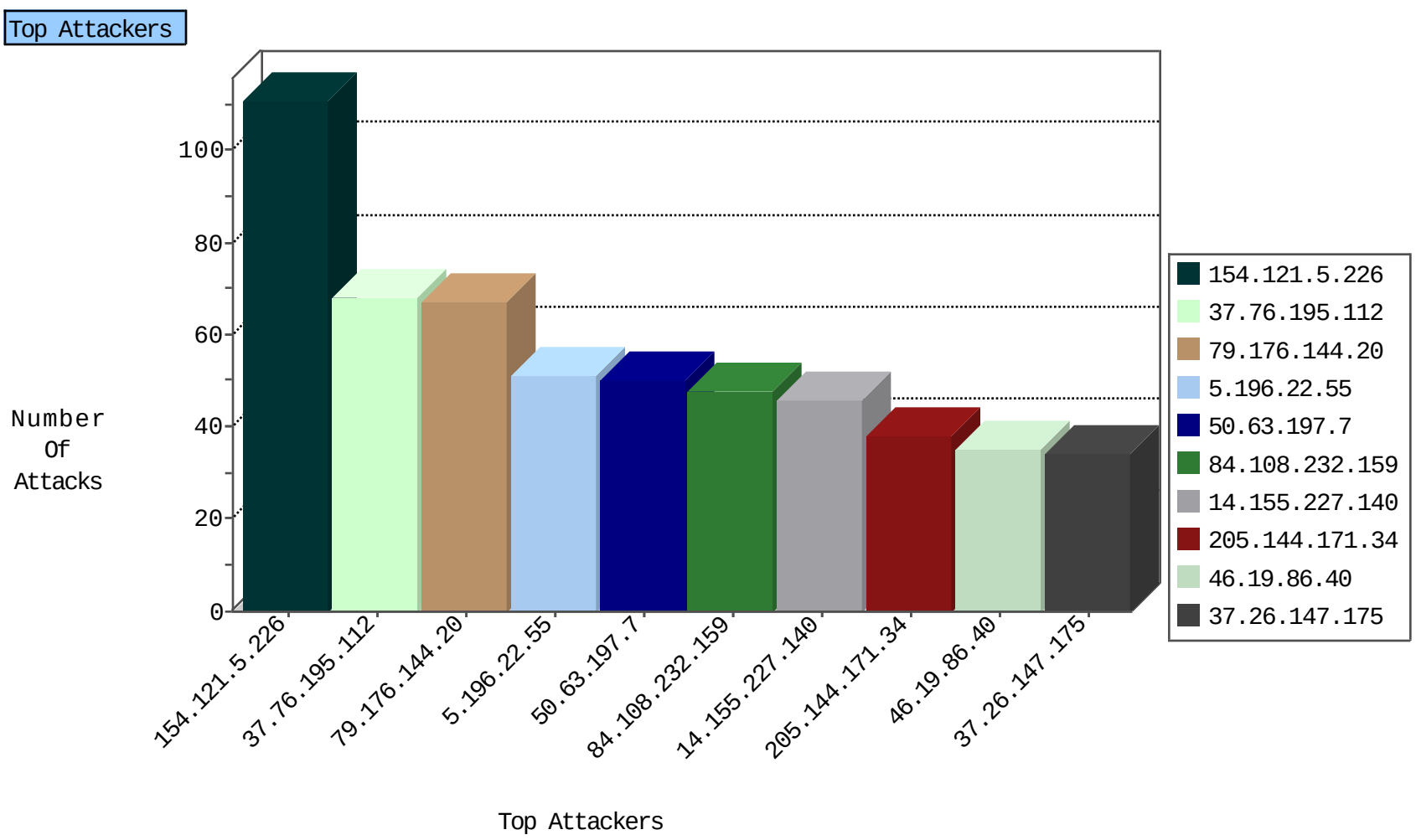
09-21-2016-22:04:02 to 09-21-2016-23:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-21-2016-22:04:02 to 09-21-2016-23:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.140.27	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
109.253.141.213	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
173.208.197.206	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
222.186.21.97	China	147.237.76.39	mobile.meitav.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
185.94.111.1	Russian Federation	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
63.141.242.197	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	1
45.32.196.8	United States	147.237.76.34	yohalan.idf.il	Black List	drop	1
218.93.206.21	China	147.237.76.39	mobile.meitav.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
69.30.226.219	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
45.32.201.228	Netherlands	147.237.76.44	e.refuah.idf.il	Black List	drop	1
109.65.4.192	Israel	147.237.72.166	aka.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.30	himush.idf.il	Black List	drop	1
63.141.231.195	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	1

09-21-2016-22:04:02 to 09-21-2016-23:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.196.22.55	France	147.237.77.226	www.chamatz.aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
50.63.197.7	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
178.137.84.187	Ukraine	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Permit	8
5.196.22.55	France	147.237.77.226	www.chamatz.aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.197.143	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
205.144.171.34	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.151.208.90	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
205.144.171.34	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
50.63.197.7	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
177.12.161.72	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.197.7	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
205.144.171.34	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6

09-21-2016-22:04:02 to 09-21-2016-23:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.196.22.55	147.237.77.226	France	www.chamatz.aka.idf.il	SQL Injection - Select From	33
50.63.197.7	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	26
205.144.171.34	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	20
177.12.161.72	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	18
50.63.197.143	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	8
91.151.208.90	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	8
123.141.236.69	147.237.72.156	Korea, Republic of	aman.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	3
164.52.227.101	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
218.93.206.21	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
218.93.206.21	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
104.167.6.84	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
45.40.135.12	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.93.206.21	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.151	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
23.91.75.231	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
218.93.206.21	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.151	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	1
192.151.154.43	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 4096	1
94.102.56.151	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
183.204.99.188	147.237.77.235	China	sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.64.117	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
61.240.144.65	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
164.52.227.101	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
164.52.227.101	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
218.93.206.21	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
110.5.109.236	147.237.77.235	Indonesia	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
45.40.135.12	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 2048	1
218.93.206.21	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
104.167.6.84	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
45.40.135.12	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -f -sS	1
218.93.206.21	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.151	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.151	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
192.151.154.43	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 3072	1
183.80.100.233	147.237.8.14	Vietnam	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.240.144.65	147.237.77.234	China	halag.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
175.103.58.114	147.237.76.30	Indonesia	himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.77.74	China	law.idf.il	ET SCAN Potential VNC Scan 5800-5820	1

09-21-2016-22:04:02 to 09-21-2016-23:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.76.195.112	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
154.121.5.226	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
109.253.131.230	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	25
154.121.5.226	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
188.161.61.108	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
154.121.5.226	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.86.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
109.253.206.222	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
37.26.147.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
154.121.5.226	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.86.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
154.121.5.226	Algeria	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
154.121.5.226	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	9
46.116.1.156	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
109.253.131.230	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
109.253.206.222	Israel	147.237.72.166	aka.idf.il	SYN Attack		monitor	8
79.178.104.137	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.131	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.86.18	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
79.177.203.190	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
93.173.72.108	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.86.18	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
93.173.72.108	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
37.26.147.175	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
80.246.137.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.111.104.92	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
185.120.125.11	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.138.73	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.253.218.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
176.13.239.33	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
37.26.147.205	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.120.144.35	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.40	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	5
154.121.5.226	Algeria	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
85.130.232.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
154.121.5.226	Algeria	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
154.121.5.226	Algeria	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
37.26.147.175	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
207.241.226.144	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
37.26.147.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
80.246.138.73	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.76	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.116.1.156	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
37.26.147.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.64.136.102	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.239.33	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4

09-21-2016-22:04:02 to 09-21-2016-23:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.176.144.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
84.108.232.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
14.155.227.140	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 14.155.227.140	Block	17
14.155.227.140	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 14.155.227.140	Block	16
46.19.86.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
14.155.227.140	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
14.155.227.140	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	6
5.29.51.225	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/faq/faq.aspx	Block	5
77.125.87.136	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	5
109.253.204.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.135.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.126.0.56	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.126.0.56	Block	3
85.65.194.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.228.36.95	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
77.237.138.202	Czech Republic	147.237.77.235	sviva.idf.il	Unauthorized Method HEAD for /	Block	1
66.249.79.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1129-he/dover.aspx	Block	1
62.0.117.253	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
2.53.138.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
77.126.0.56	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/kapatz/	Block	1
66.249.64.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
68.180.228.44	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
95.143.213.229	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
77.138.113.154	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
66.249.64.142	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3208.pdf	Block	1
14.155.227.140	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
79.181.200.123	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/booklets.aspx	Block	1
77.138.168.251	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	1
66.249.64.181	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
77.126.0.56	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
157.55.39.102	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1
77.139.119.38	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.64.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.120.144.35	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
85.64.179.145	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.240.192.138	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to 147.237.76.147/robots.txt	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/404.aspx	Block	1

09-21-2016-22:04:02 to 09-21-2016-23:04:02