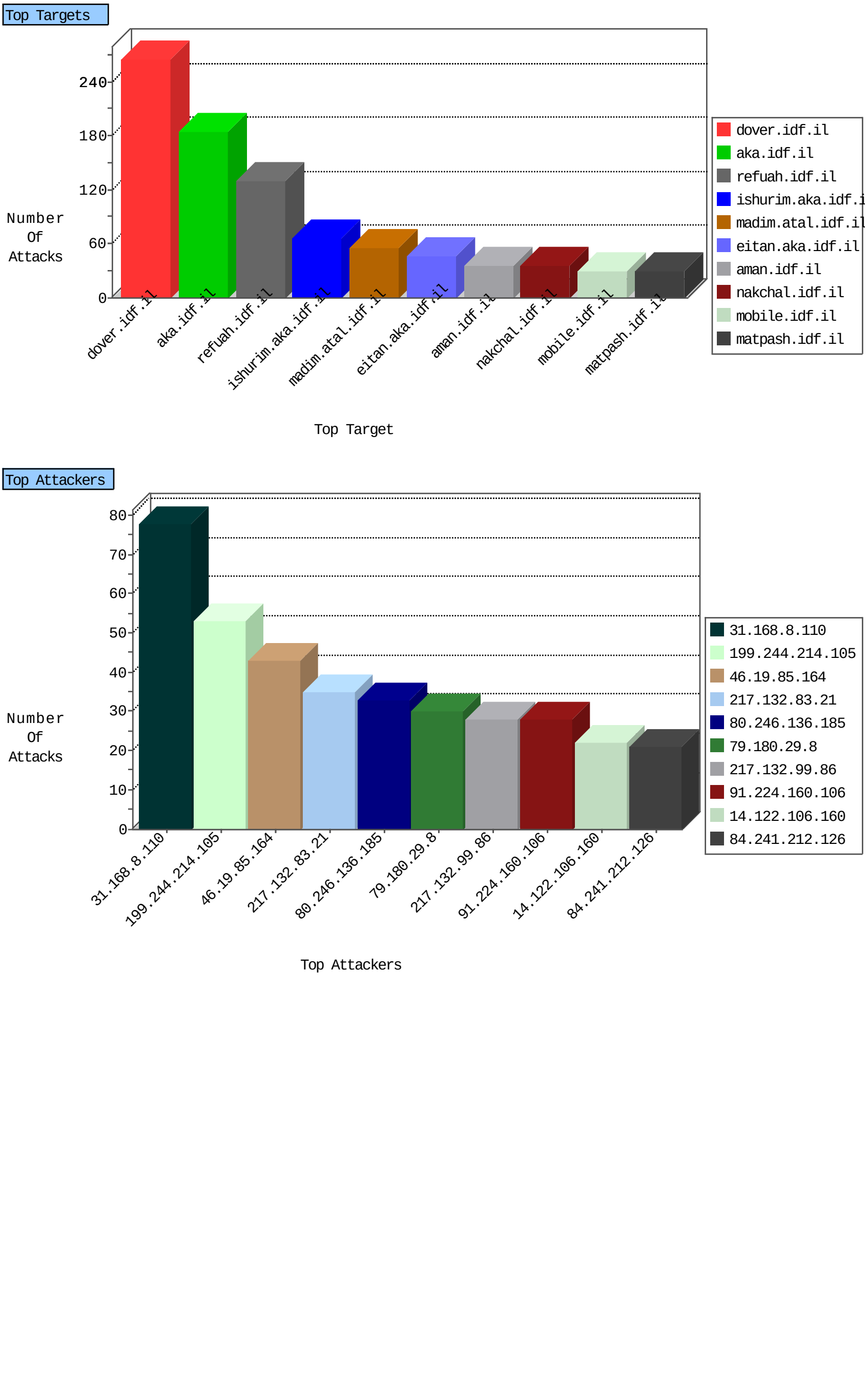
09-13-2016-16:04:00 to 09-13-2016-17:04:00

IDF Under Attack Daily Report



09-13-2016-16:04:00 to 09-13-2016-17:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
88.65.147.114	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
109.253.159.239	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.1.13.12	Ireland	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
46.19.86.123	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.13	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-13-2016-16:04:00 to 09-13-2016-17:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.108.60.106	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-13-2016-16:04:00 to 09-13-2016-17:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.164	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	22
91.224.160.106	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
5.255.90.133	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
89.189.227.48	147.237.77.216	Saudi Arabia	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.13.196	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.29.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
84.94.184.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.93.234.8	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
2.53.161.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
186.118.239.206	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.93.87	147.237.77.216	Europe	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential SSH Scan	1
138.201.132.254	147.237.0.33	Germany	idf.il	ET SCAN NMAP -sS window 1024	1
52.166.249.197	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
91.208.139.250	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.93.225	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.116.72.226	147.237.77.212	Sweden	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
2.55.1.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
67.211.219.120	147.237.77.227	United States	e.hamaz.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
195.88.208.193	147.237.0.15	Russian Federation	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1
186.113.163.119	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.64.113	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
91.224.160.106	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	1
109.139.69.36	147.237.77.216	Belgium	dover.idf.il	portscan: TCP Distributed Portscan	1
52.166.249.197	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	1

09-13-2016-16:04:00 to 09-13-2016-17:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
199.244.214.105	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
217.132.99.86	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
79.180.29.8	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
84.241.212.126	Netherlands	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
217.132.83.21	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
217.132.83.21	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
2.53.8.120	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.173	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
130.193.51.3	Russian Federation	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
79.180.29.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.85.164	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
109.66.10.145	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.98	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.253.223.62	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
199.244.214.105	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN-ACK was acknowledged. Stripping all packet data.	drop	6
185.32.179.134	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
2.53.182.81	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
37.26.147.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.226.218.52	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.185	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.53.4.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.98	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
199.244.214.105	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
46.19.86.171	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
176.13.229.35	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.123	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
85.64.116.79	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.171	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.123	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
112.204.202.73	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.13	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.48	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.179.175.62	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
213.57.199.147	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
2.55.27.17	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.128.80	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
199.244.214.105	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
79.182.134.197	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
37.26.147.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.175	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.185	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.117.157.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
46.19.86.98	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
142.4.206.228	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3

09-13-2016-16:04:00 to 09-13-2016-17:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.168.8.110	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	41
31.168.8.110	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 31.168.8.110	Block	34
80.246.136.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
14.122.106.160	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 14.122.106.160	Block	15
2.53.191.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
84.109.160.171	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	8
37.26.147.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
14.122.106.160	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	6
46.19.85.57	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	4
31.168.8.110	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/1/	Block	3
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.105	Block	2
217.132.44.28	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 217.132.44.28	Block	2
46.121.40.183	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.55.44.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.117.19.180	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.145.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.179.19.71	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl51 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
5.29.179.142	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.102.9.22	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	1
46.19.86.48	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method 8.fd1c=bf372e3ec9b30f61.1455710578.8.1473715752.1473715752.; in URL asp.net_sessionid=amoumo2peoide245tsij15us	Block	1
46.19.85.238	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
82.81.160.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	1
77.125.7.37	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
46.120.134.57	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
192.118.10.10	Israel	147.237.72.166	aka.idf.il	Cookie Tampering on cookie wb48617274: Expected 56AFE102, Observed 1844EB31	None	1
46.19.86.29	Israel	147.237.77.226	www.chamatz.aka.idf.il	Illegal HTTP Version /Shared/ClientScripts/Swiper/swiper.jquery.js HTTP/1.1	Block	1
79.180.29.8	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
40.77.167.81	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.19.86.98	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.85.238	Israel	147.237.77.216	dover.idf.il	Malformed URL he-il,he;q=0.8,en-us;q=0.6,en;q=0.4	Block	1
77.138.133.62	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
200.111.107.58	Chile	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/index.php	Block	1
46.19.86.48	Israel	147.237.76.42	refuah.idf.il	Abnormally Long Request request version	Block	1
79.180.56.184	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
41.60.25.38	Zambia	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
66.249.64.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/.well-known/assetlinks.json	Block	1
46.116.67.101	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.238	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method t-Language: in URL he-il,he	Block	1
87.70.30.68	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giys	Block	1
77.138.160.26	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/information.aspx	Block	1
46.121.92.148	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 46.121.92.148 (Unknown SSL Session)	None	1
207.46.13.64	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
46.19.86.48	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version __atuvc=0%7C33%2C0%7C34%2C0%7C35%2C0%7C36%2C4%7C37; __atuvs=57d7fb8fa4e6830c000	Block	1
14.122.106.160	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.asp	Block	1
66.249.64.113	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.86.29	Israel	147.237.77.226	www.chamatz.aka.idf.il	Abnormally Long Request request version	Block	1
79.139.232.164	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
37.26.147.161	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1

09-13-2016-16:04:00 to 09-13-2016-17:04:00