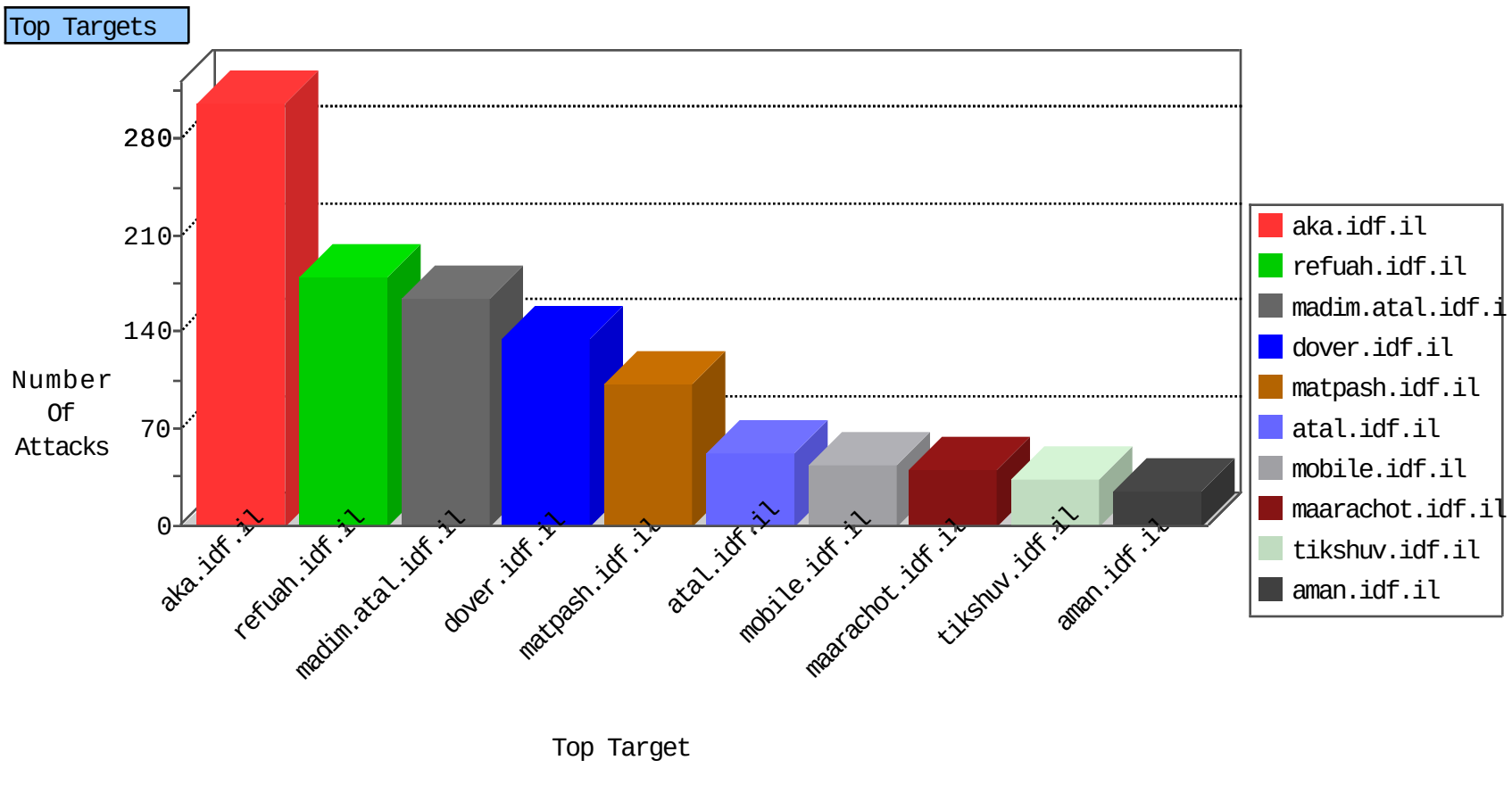
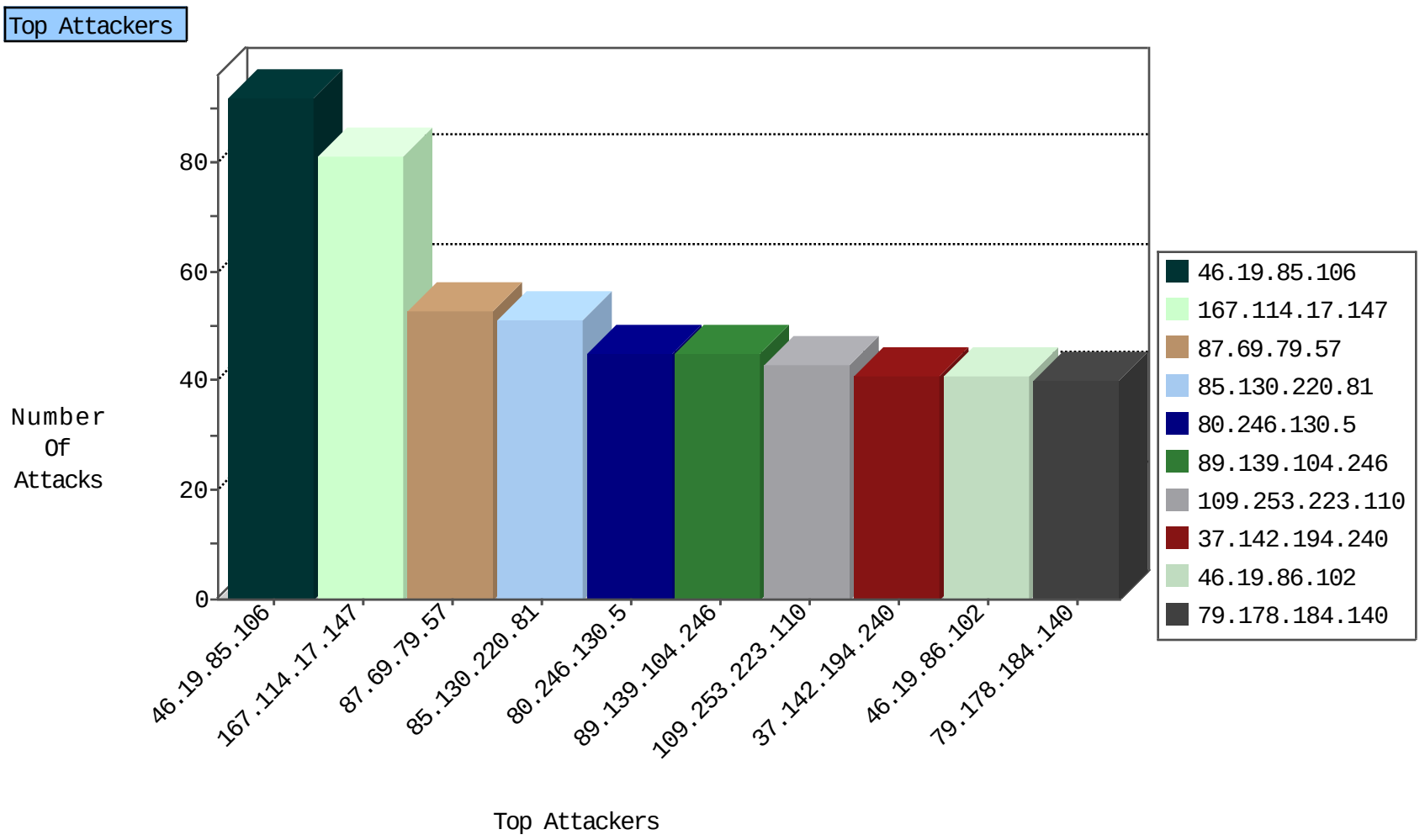
09-17-2016-21:04:00 to 09-17-2016-22:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-17-2016-21:04:00 to 09-17-2016-22:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	9
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	7
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.97.74.14	Canada	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	2
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
131.179.150.72	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	2
128.208.4.99	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	2
176.13.250.113	Israel	147.237.0.19	madim.atal.idf.il	DOSS-SSL-ClearText	drop	1
128.8.126.111	United States	147.237.72.166	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
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.82	Czech Republic	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.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
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-17-2016-21:04:00 to 09-17-2016-22:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.116.197	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	8
46.4.116.197	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	3

09-17-2016-21:04:00 to 09-17-2016-22:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.84	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
91.201.236.50	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
77.138.65.53	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.50	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -f -sS	1
91.201.236.50	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
91.197.232.15	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN Potential SSH Scan	1
201.38.68.132	147.237.77.61	Brazil	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
91.197.232.15	147.237.76.200	Russian Federation	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
185.93.242.67	147.237.8.28	Poland	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.197.232.15	147.237.76.34	Russian Federation	yohalan.idf.il	ET SCAN Potential SSH Scan	1
177.99.218.218	147.237.0.33	Brazil	idf.il	ET SCAN NMAP -sS window 3072	1
91.197.232.15	147.237.0.15	Russian Federation	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
113.74.58.157	147.237.76.201	China	e.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.193.74.175	147.237.76.196	Gibraltar	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
104.167.6.84	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
36.77.52.148	147.237.76.44	Indonesia	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.50	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
91.197.232.15	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
202.155.58.28	147.237.77.235	Indonesia	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
91.197.232.15	147.237.76.202	Russian Federation	e.halag.idf.il	ET SCAN Potential SSH Scan	1
192.223.72.226	147.237.72.166	Bolivia	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.197.232.15	147.237.76.199	Russian Federation	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
179.43.141.228	147.237.0.15	Switzerland	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.197.232.15	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
124.107.133.189	147.237.76.200	Philippines	eitan.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.193.74.175	147.237.77.235	Gibraltar	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
109.64.187.14	147.237.77.216	Israel	dover.idf.il	ET SCAN NMAP -sA (2)	1
85.120.95.119	147.237.76.176	Romania	test.ncore.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

09-17-2016-21:04:00 to 09-17-2016-22:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.17.147	Canada	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	81
87.69.79.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	53
80.246.130.5	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	44
89.139.104.246	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	44
95.35.71.65	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
46.19.85.123	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
46.19.85.34	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
46.19.85.34	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
79.178.165.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
46.19.85.123	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
37.142.194.240	Israel	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Response out of state	monitor	12
85.130.220.81	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
80.246.130.84	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.224	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.86.102	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.85.224	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
85.130.220.81	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
85.130.220.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
85.130.220.81	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.244	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
85.130.220.81	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
46.19.86.244	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.142.194.240	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
85.130.220.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.53.30.137	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
109.67.157.153	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
80.246.130.84	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.102	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
109.253.245.140	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.194.240	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence		monitor	6
31.154.81.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.137.243	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.55	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.199	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
79.178.165.67	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
109.65.128.46	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.76.205.68	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
79.178.165.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.55.131.131	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.120.129.110	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
109.253.223.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
2.55.20.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
37.142.194.240	Israel	147.237.77.170	maarachot.idf.il	Multiple Abnormally Long Request from 37.142.194.240	Block	11
2.53.12.109	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.53.12.109	Block	5
84.109.75.161	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
79.178.184.140	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 79.178.184.140	Block	3
109.253.207.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.184.140	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 79.178.184.140	Block	3
79.178.184.140	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 79.178.184.140	Block	3
79.178.184.140	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 79.178.184.140	Block	3
176.13.250.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.184.140	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 79.178.184.140	Block	3
2.53.12.109	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
79.178.184.140	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 79.178.184.140	Block	2
79.178.184.140	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 79.178.184.140	Block	2
37.26.149.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.127.88.26	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	2
79.178.184.140	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 79.178.184.140	Block	2
79.178.184.140	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
37.26.146.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
141.226.161.154	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
79.178.184.140	Israel	147.237.72.166	aka.idf.il	Malformed URL eา¿oaʅs'x•˛˛"	Block	1
79.177.222.57	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
79.178.184.140	Israel	147.237.72.166	aka.idf.il	NULL Character in Method sõ4[[#0]]j‹[[#29]]ë®!ãmÒó¬-ë•[[#17]],ºMu&©L[[#22]]©Ö‹&ëOÑwÕ[[#15]] qµT[[#31]]·“"w¨[[#14]]ÅS[[#14]]Ý4[[#26]][[#28]].€Ž[[#7]]5*[[#3]];fkœöÇc	Block	1
71.6.167.142	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/robots.txt	Block	1
212.117.128.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.66.134.88	Israel	147.237.72.166	aka.idf.il	Unknown Parameter answerid in www.aka.idf.il/sachar/login/	None	1
79.178.184.140	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
79.181.12.246	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
77.139.173.230	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
60.217.192.136	China	147.237.77.216	dover.idf.il	Unauthorized Method HEAD for 147.237.77.216/	Block	1
148.251.13.51	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
79.178.184.140	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
89.139.104.246	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
79.178.184.140	Israel	147.237.72.166	aka.idf.il	NULL Character in URL jÚg˛˛[[#12]]Œ=•^û[[#27]]dλy″-`œ„…|•‸£2¶□5j'ı" 2:[[#0]]m€(	Block	1
46.116.51.10	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.53.141.136	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie Login: Expected ** ** ** **********, Observed ** ** ** ****	None	1
79.178.184.140	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method €[[#6]]tT	Block	1
77.139.200.153	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
80.246.130.5	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
62.90.94.129	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
37.142.194.240	Israel	147.237.77.170	maarachot.idf.il	Abnormally Long Request query string	Block	1
157.55.39.122	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
79.178.184.140	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
95.35.71.65	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
79.178.184.140	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
77.138.80.38	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
46.120.67.169	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1050-he/pickcertificates.aspx	Block	1
79.178.184.140	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 79.178.184.140	Block	1