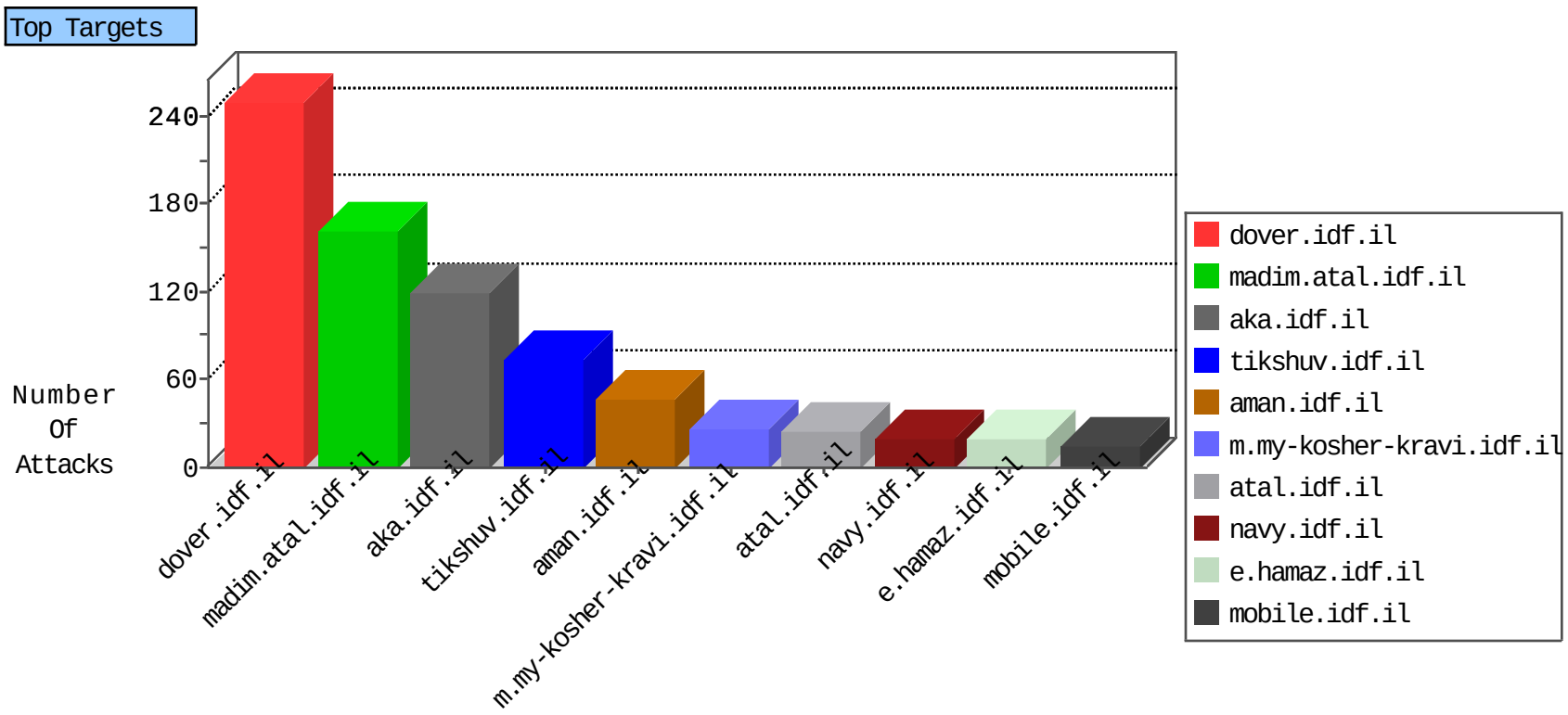
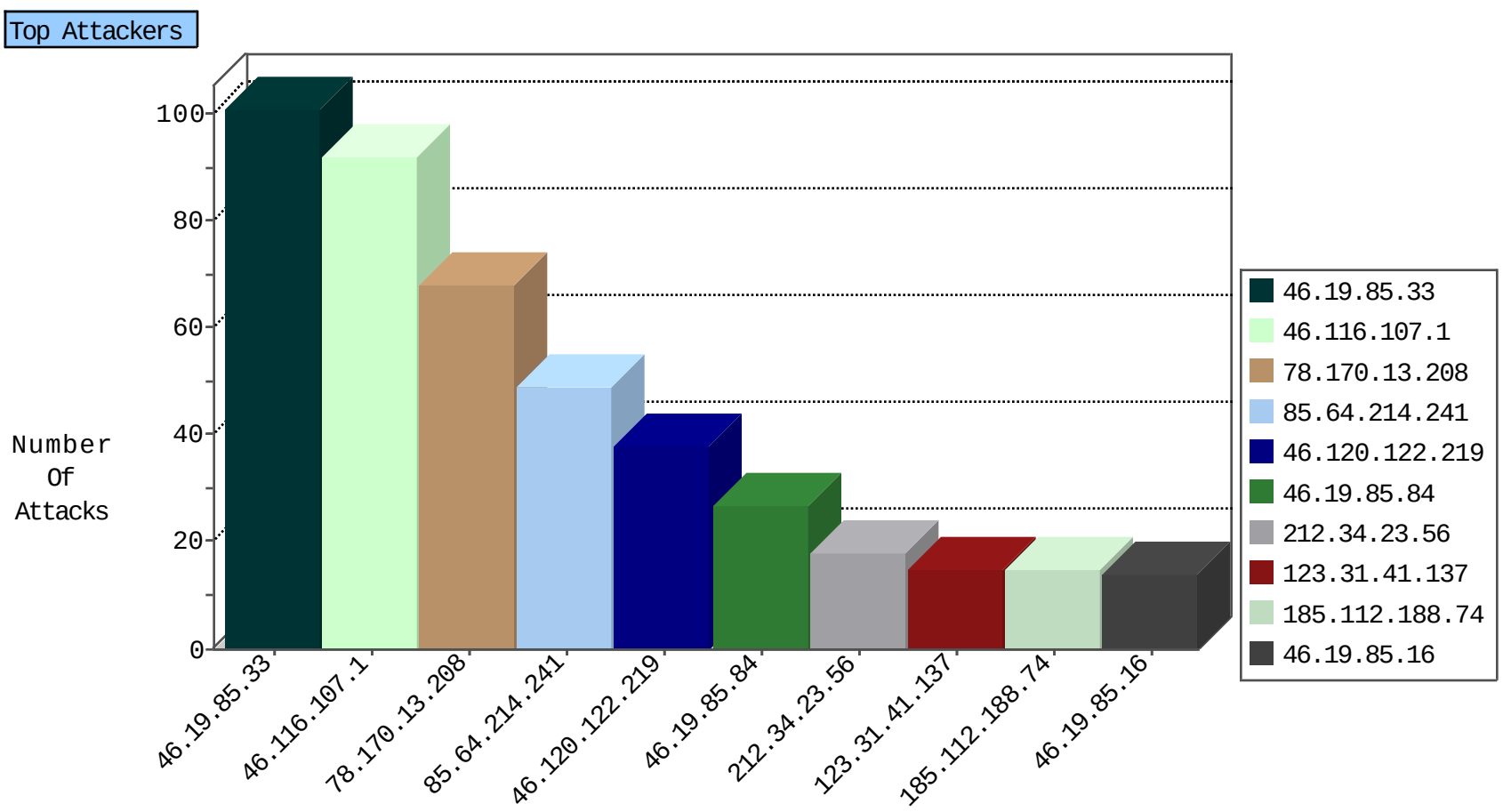
09-30-2016-20:04:04 to 09-30-2016-21:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-30-2016-20:04:04 to 09-30-2016-21:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.11.5	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
81.218.15.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
2.53.4.43	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
194.177.16.3	Israel	147.237.76.86	navy.idf.il	Black List	drop	3
93.158.200.126	Netherlands	147.237.76.198	e.yohalan.idf.il	Black List	drop	1

09-30-2016-20:04:04 to 09-30-2016-21:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-30-2016-20:04:04 to 09-30-2016-21:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.0.17	Israel	m.my-kosher-kravi.idf.il	Xenu Link Sleuth User Agent	24
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	8
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	4
123.31.41.137	147.237.0.200	Vietnam	m4u.idf.il	ET SCAN Potential SSH Scan	2
151.80.41.96	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
123.31.41.137	147.237.77.227	Vietnam	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
123.31.41.137	147.237.72.166	Vietnam	aka.idf.il	ET SCAN Potential SSH Scan	2
163.172.169.150	147.237.77.19	United Kingdom	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
24.105.159.242	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
109.67.239.218	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	1
128.199.138.35	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
104.207.141.110	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1
123.31.41.137	147.237.77.226	Vietnam	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
123.31.41.137	147.237.77.176	Vietnam	matpash.idf.il	ET SCAN Potential SSH Scan	1
66.249.93.153	147.237.77.170	Europe	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
123.31.41.137	147.237.76.147	Vietnam	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
58.219.40.205	147.237.76.34	China	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.218.200.137	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
123.31.41.137	147.237.0.33	Vietnam	idf.il	ET SCAN Potential SSH Scan	1
123.31.41.137	147.237.0.15	Vietnam	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
113.103.161.204	147.237.76.177	China	ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.207.141.110	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.158	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
123.31.41.137	147.237.77.179	Vietnam	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -f -sS	1
123.31.41.137	147.237.77.19	Vietnam	law-forum.idf.il	ET SCAN Potential SSH Scan	1
66.249.64.10	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
58.218.200.137	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
123.31.41.137	147.237.0.34	Vietnam	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
54.144.119.103	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
123.31.41.137	147.237.0.17	Vietnam	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
113.240.250.154	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1

09-30-2016-20:04:04 to 09-30-2016-21:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
78.170.13.208	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
46.19.85.33	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
46.19.85.33	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	21
46.19.85.33	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
46.19.85.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
46.117.162.122	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
185.112.188.74	Iraq	147.237.77.227	e.hamaz.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.33	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
155.254.239.33	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.33	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	10
5.29.22.197	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
87.212.149.31	Netherlands	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
80.246.137.235	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
176.13.3.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.1	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.1	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.84	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.116.166.6	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.166.186.249	Netherlands	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
66.102.8.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.84	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.16	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.84	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.211	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
68.150.53.25	Canada	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.85.16	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.215	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
212.34.23.56	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
217.69.136.210	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.34.23.56	Jordan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.28.141.162	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	4
46.19.85.84	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.34.23.56	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
176.13.229.21	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.4.129.170	Cyprus	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
66.102.8.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.34.23.56	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
46.19.85.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.177.106.143	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
37.26.148.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
81.218.15.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.116.11.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

09-30-2016-20:04:04 to 09-30-2016-21:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.116.107.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
85.64.214.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
79.179.132.189	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	12
213.8.204.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
90.194.241.191	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	4
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
79.181.222.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.138.136.13	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	3
46.19.85.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.219.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.54.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.138.245.28	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	2
109.64.100.34	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	2
77.138.75.67	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.64.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1247-he/atal.aspx	Block	1
66.249.66.103	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/mobile/	Block	1
46.117.162.122	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
89.139.162.119	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
77.138.128.52	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
66.249.65.10	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1766	Block	1
125.77.28.26	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
38.104.99.190	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
81.4.129.170	Cyprus	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.149	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1093-7963-he/|שחמו מאיר.aspx	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	1
89.237.100.245	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 89.237.100.245	Block	1
66.249.65.58	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2977.jpg	Block	1
81.4.129.178	Cyprus	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/rights/	Block	1
66.249.65.59	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2827.jpg	Block	1
213.8.204.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
46.19.85.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.53.204	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
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
66.249.65.60	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/3272.jpg	Block	1

09-30-2016-20:04:04 to 09-30-2016-21:04:04